GE Consumer & Industrial
Multilin

MultiLink ML2400
Ethernet Communications Switch
Instruction Manual

Firmware Revision 3.x

Manual P/N: 1601-0220-AB
Manual Order Code: GEK-113042K

Copyright © 2008 GE Multilin

GE Multilin
215 Anderson Avenue, Markham, Ontario
Canada L6E 1B3
Tel: (905) 294-6222 Fax: (905) 201-2098
Internet: http://www.GEmultilin.com

GE Multilin's Quality Management System is registered to ISO9001:2000

QMI # 005094
UL # A3775

These instructions do not purport to cover all details or variations in equipment nor provide for every possible contingency to be met in connection with installation, operation, or maintenance. Should further information be desired or should particular problems arise which are not covered sufficiently for the purchaser's purpose, the matter should be referred to the General Electric Company.

To the extent required the products described herein meet applicable ANSI, IEEE, and NEMA standards; but no such assurance is given with respect to local codes and ordinances because they vary greatly.

© 2008 GE Multilin Incorporated. All rights reserved.

GE Multilin Multilink ML2400 instruction manual for revision 3.x.

Multilink ML2400 is a registered trademark of GE Multilin Inc.

The contents of this manual are the property of GE Multilin Inc. This documentation is furnished on license and may not be reproduced in whole or in part without the permission of GE Multilin. The content of this manual is for informational use only and is subject to change without notice.

Part numbers contained in this manual are subject to change without notice, and should therefore be verified by GE Multilin before ordering.

Part number: 1601-0220-AB (June 2008)

Table of Contents

1: INTRODUCTION

GETTING STARTED 1-1
- INSPECTING THE PACKAGE AND PRODUCT 1-1

ORDERING 1-2
- ORDER CODES 1-2

SPECIFICATIONS 1-3
- TECHNICAL SPECIFICATIONS 1-3
- ENVIRONMENTAL SPECIFICATIONS 1-5
- TYPE TESTS 1-5
- PHYSICAL SPECIFICATIONS 1-6
- APPROVALS AND WARRANTY 1-6

FIRMWARE OVERVIEW 1-8
- COMMAND LINE FIRMWARE 1-8
- ENERVISTA SOFTWARE 1-8
- BEFORE STARTING 1-9

COMMAND LINE INTERFACE FIRMWARE 1-10
- CONSOLE CONNECTION 1-10
- CONSOLE SETUP 1-10
- CONSOLE SCREEN 1-11
- LOGGING IN FOR THE FIRST TIME 1-11
- AUTOMATIC IP ADDRESS CONFIGURATION 1-11
- SETTING THE IP PARAMETERS 1-12
- PRIVILEGE LEVELS 1-14
- USER MANAGEMENT 1-14
- HELP 1-15
- EXITING 1-17

ENERVISTA SECURE WEB MANAGEMENT 1-18
- LOGGING IN FOR THE FIRST TIME 1-18
- PRIVILEGE LEVELS 1-19
- USER MANAGEMENT 1-19
- MODIFYING THE PRIVILEGE LEVEL 1-22
- HELP 1-22
- EXITING 1-23

ML2400 FIRMWARE UPDATES 1-24
- UPDATING MULTILINK FIRMWARE 1-24
- SELECTING THE PROPER VERSION 1-24
- UPDATING THROUGH THE COMMAND LINE 1-24
- UPDATING THROUGH THE ENERVISTA SOFTWARE 1-25

2: PRODUCT DESCRIPTION

OVERVIEW 2-1
- INTRODUCTION TO THE ML2400 2-1
- DESIGN ASPECTS 2-2

COMMUNICATIONS MODULES 2-3
- FOUR-PORT MODULES 2-3
- SIX-PORT MODULES 2-4
- EIGHT-PORT MODULES 2-4
- GIGABIT (1000 MBPS) MODULES 2-6

FEATURES AND BENEFITS 2-7
- PACKET PRIORITIZATION, 802.1P QOS 2-7
- FRAME BUFFERING AND FLOW CONTROL 2-7

MULTILINK SWITCH SOFTWARE 2-7
REDUNDANT POWER SUPPLY 2-8
ADDITIONAL FEATURES AND BENEFITS 2-8
APPLICATIONS 2-10
DESCRIPTION 2-10
ML2400 SWITCH FOR A VLAN APPLICATION 2-10
NETWORK WITH MULTIPLE SUBNETS 2-11

3: INSTALLATION
PREPARATION 3-1
PRECAUTIONS 3-1
LOCATING THE ML2400 3-1
CONNECTING ETHERNET MEDIA 3-3
DESCRIPTION 3-3
CONNECTING ST-TYPE FIBER OPTICS (TWIST-LOCK) 3-3
CONNECTING SC-TYPE FIBER OPTICS (SNAP-IN) 3-4
CONNECTING SINGLE-MODE FIBER OPTICS 3-4
CONNECTING RJ45 TWISTED PAIR 3-4
CONNECTING GIGABIT MEDIA USING GBICS 3-5
MECHANICAL INSTALLATION 3-6
TABLE-TOP OR SHELF MOUNTING 3-6
RACK MOUNTING 3-6
ELECTRICAL INSTALLATION 3-8
POWERING THE ML2400 3-8
UL REQUIREMENTS FOR DC-POWERED UNITS 3-8
ALARM CONTACTS 3-9
DIELECTRIC STRENGTH (HI-POT) TESTING 3-10
CONNECTING A MANAGEMENT CONSOLE TERMINAL TO THE ML2400 3-11
DESCRIPTION 3-11

4: OPERATION
FUNCTIONALITY 4-1
SWITCHING FUNCTIONALITY 4-1
FILTERING AND FORWARDING 4-1
ADDRESS LEARNING 4-2
STATUS LEDS 4-2
UP-LINK MANUAL SWITCHES (FOR RJ45 PORT ONLY) 4-2
AUTO-NEGOTIATION (FOR FAST ETHERNET COPPER PORTS) 4-2
FLOW CONTROL (IEEE 802.3X) 4-3
POWER BUDGET CALCULATIONS WITH FIBER MEDIA 4-5
TROUBLESHOOTING 4-7
OVERVIEW 4-7
BEFORE CALLING FOR ASSISTANCE 4-7
WHEN CALLING FOR ASSISTANCE 4-7

5: IP ADDRESSING
IP ADDRESS AND SYSTEM INFORMATION 5-1
OVERVIEW 5-1
IMPORTANCE OF AN IP ADDRESS 5-3
DHCP AND BOOTP 5-3
BOOTP DATABASE 5-3
CONFIGURING DHCP/BOOTP/MANUAL/AUTO 5-3
USING TELNET 5-5
SETTING PARAMETERS 5-8

SETTING SERIAL PORT PARAMETERS 5-8
SYSTEM PARAMETERS 5-8
DATE AND TIME 5-9
NETWORK TIME 5-10
SYSTEM CONFIGURATION 5-13
SAVING AND LOADING – COMMAND LINE 5-13
CONFIG FILE 5-13
DISPLAYING CONFIGURATION 5-16
SAVING CONFIGURATION 5-19
SCRIPT FILE 5-21
SAVING AND LOADING – ENERVISTA SOFTWARE 5-22
HOST NAMES 5-24
ERASING CONFIGURATION 5-25
IPV6 5-29
INTRODUCTION TO IPV6 5-29
WHAT'S CHANGED IN IPV6? 5-29
IPV6 ADDRESSING 5-30
CONFIGURING IPV6 5-31
LIST OF COMMANDS IN THIS CHAPTER 5-32

6: ACCESS CONSIDERATIONS
SECURING ACCESS 6-1
DESCRIPTION 6-1
PASSWORDS 6-1
PORT SECURITY FEATURE 6-2
CONFIGURING PORT SECURITY THROUGH THE COMMAND LINE INTERFACE 6-3
COMMANDS 6-3
SECURITY LOGS 6-8
AUTHORIZED MANAGERS 6-10
CONFIGURING PORT SECURITY WITH ENERVISTA SOFTWARE 6-12
COMMANDS 6-12
LOGS 6-14
AUTHORIZED MANAGERS 6-15

7: ACCESS USING RADIUS
INTRODUCTION TO 802.1X 7-1
DESCRIPTION 7-1
802.1X PROTOCOL 7-1
CONFIGURING 802.1X THROUGH THE COMMAND LINE INTERFACE 7-4
COMMANDS 7-4
EXAMPLE 7-6
CONFIGURING 802.1X WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 7-9
COMMANDS 7-9

8: ACCESS USING TACACS+
INTRODUCTION TO TACACS+ 8-1
OVERVIEW 8-1
TACACS+ FLOW 8-2
TACACS+ PACKET 8-2
CONFIGURING TACACS+ THROUGH THE COMMAND LINE INTERFACE 8-4
COMMANDS 8-4
EXAMPLE 8-4

CONFIGURING TACACS+ WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 8-6

9: PORT MIRRORING AND SETUP

PORT MIRRORING 9-1
DESCRIPTION 9-1
PORT MIRRORING USING THE COMMAND LINE INTERFACE 9-2
COMMANDS 9-2
PORT SETUP 9-3
COMMANDS 9-3
FLOW CONTROL 9-5
BACK PRESSURE 9-5
BROADCAST STORMS 9-8
LINK LOSS ALERT 9-10
PORT MIRRORING USING ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 9-12
COMMANDS 9-12
PORT SETUP 9-13
BROADCAST STORMS 9-15

10: VLAN

VLAN DESCRIPTION 10-1
OVERVIEW 10-1
TAG VLAN VS. PORT VLAN 10-3
CONFIGURING PORT VLANS THROUGH THE COMMAND LINE INTERFACE 10-4
DESCRIPTION 10-4
COMMANDS 10-4
EXAMPLE 10-5
CONFIGURING PORT VLANS WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 10-9
DESCRIPTION 10-9
CONFIGURING TAG VLANS THROUGH THE COMMAND LINE INTERFACE 10-13
DESCRIPTION 10-13
COMMANDS 10-13
EXAMPLE 10-14
CONFIGURING TAG VLANS WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 10-20
DESCRIPTION 10-20

11: VLAN REGISTRATION OVER GARP

OVERVIEW 11-1
DESCRIPTION 11-1
GVRP CONCEPTS 11-1
GVRP OPERATIONS 11-2
CONFIGURING GVRP THROUGH THE COMMAND LINE INTERFACE 11-7
COMMANDS 11-7
GVRP OPERATION NOTES 11-7
CONFIGURING GVRP WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 11-9
EXAMPLE 11-9

12: SPANNING TREE PROTOCOL (STP)

OVERVIEW 12-1
DESCRIPTION 12-1

FEATURES AND OPERATION 12-1
CONFIGURING STP 12-3

13: RAPID SPANNING TREE PROTOCOL
OVERVIEW 13-1
DESCRIPTION 13-1
RSTP CONCEPTS 13-1
TRANSITION FROM STP TO RSTP 13-2
CONFIGURING RSTP THROUGH THE COMMAND LINE INTERFACE 13-4
NORMAL RSTP 13-4
SMART RSTP (RING-ONLY MODE) THROUGH THE COMMAND LINE INTERFACE 13-14
CONFIGURING STP/RSTP WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 13-16
NORMAL RSTP 13-16
SMART RSTP (RING-ONLY MODE) WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 13-20

14: QUALITY OF SERVICE
QOS OVERVIEW 14-1
DESCRIPTION 14-1
QOS CONCEPTS 14-1
DIFFSERV AND QOS 14-2
IP PRECEDENCE 14-2
CONFIGURING QOS THROUGH THE COMMAND LINE INTERFACE 14-4
COMMANDS 14-4
EXAMPLE 14-6
CONFIGURING QOS WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 14-9
DESCRIPTION 14-9

15: IGMP
OVERVIEW 15-1
DESCRIPTION 15-1
IGMP CONCEPTS 15-1
IP MULTICAST FILTERS 15-4
RESERVED ADDRESSES EXCLUDED FROM IP MULTICAST (IGMP) FILTERING 15-5
IGMP SUPPORT 15-5
CONFIGURING IGMP THROUGH THE COMMAND LINE INTERFACE 15-6
COMMANDS 15-6
EXAMPLE 15-8
CONFIGURING IGMP WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 15-11
EXAMPLE 15-11

16: SNMP
OVERVIEW 16-1
DESCRIPTION 16-1
SNMP CONCEPTS 16-1
CONFIGURING SNMP THROUGH THE COMMAND LINE INTERFACE 16-4
COMMANDS 16-4
EXAMPLE 16-5
CONFIGURING SNMP WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 16-10
EXAMPLE 16-10

CONFIGURING RMON 16-13
DESCRIPTION 16-13
COMMANDS 16-13

17: MISCELLANEOUS COMMANDS

ALARM RELAYS 17-1
DESCRIPTION 17-1
CONFIGURING ALARM RELAYS THROUGH THE COMMAND LINE INTERFACE 17-2
CONFIGURING ALARM RELAYS WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 17-5
E-MAIL 17-6
DESCRIPTION 17-6
COMMANDS 17-6
EXAMPLE 17-8
STATISTICS 17-9
VIEWING PORT STATISTICS WITH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 17-9
SERIAL CONNECTIVITY 17-11
DESCRIPTION 17-11
HISTORY 17-12
COMMANDS 17-12
PING 17-13
PING THROUGH THE COMMAND LINE INTERFACE 17-13
PING THROUGH ENERVISTA SECURE WEB MANAGEMENT SOFTWARE 17-13
PROMPT 17-14
CHANGING THE COMMAND LINE PROMPT 17-14
SYSTEM EVENTS 17-15
DESCRIPTION 17-15
COMMAND LINE INTERFACE EXAMPLE 17-15
ENERVISTA EXAMPLE 17-16
COMMAND REFERENCE 17-18
MAIN COMMANDS 17-18
CONFIGURATION COMMANDS 17-20

18: MODBUS PROTOCOL

MODBUS CONFIGURATION 18-1
OVERVIEW 18-1
COMMAND LINE INTERFACE SETTINGS 18-1
ENERVISTA SETTINGS 18-2
MEMORY MAPPING 18-3
MODBUS MEMORY MAP 18-3
FORMAT CODES 18-36

19: APPENDIX

REVISION HISTORY 19-1
CHANGE NOTES 19-1
CHANGES TO THE MANUAL 19-2
WARRANTY 19-5
GE MULTILIN WARRANTY STATEMENT 19-5

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 1: Introduction

1.1 Getting Started

1.1.1 Inspecting the Package and Product

Examine the shipping container for obvious damage prior to installing this product; notify the carrier of any damage that you believe occurred during shipment or delivery. Inspect the contents of this package for any signs of damage and ensure that the items listed below are included.

This package should contain:

- MultiLink ML2400 Ethernet Switch, base unit (configured with user-selected port module options installed)
- Set of metal “ears” for 19-inch rack mounting
- Installation and user guide (this manual)

Remove the items from the shipping container. Be sure to keep the shipping container should you need to re-ship the unit at a later date. To validate the product warranty, please complete and return the enclosed product registration card to GE Multilin as soon as possible.

In the event there are items missing or damaged, contact the party from whom you purchased the product. If the unit needs to be returned, please use the original shipping container if possible. Refer to *Troubleshooting* on page 4–7, for specific return procedures.

1.2 Ordering

1.2.1 Order Codes

The following table illustrates the order codes for the MultiLink ML2400 Ethernet Switch.

The fiber optic LC ports are limited to a total of 12.

Table 1–1: ML2400 Order Code

ML2400 – * – * – * – * – * – * – * – *									
Module				**A**	**B**	**C**	**D**		
Base	**ML2400**								MultiLink ML2400 Ethernet Switch
Port mounting	**F**								Front-mounted ports
	B								Rear-mounted ports
Power supply		**AC**							100 to 240 V AC power supply
		HI							88 to 300 V DC / 85 to 865 V AC
		LO							36 to 70 V DC
Redundant power supply			**XX**						No redundant power supply
			HI						88 to 300 V DC / 85 to 865 V AC power supply
			LO						36 to 70 V DC power supply
Modules				**A1**	**A1**	**A1**	**A1**		4 × 10 Mb - ST mm fiber
				A2	**A2**	**A2**	**A2**		4 × 100 Mb - ST mm fiber
				A3	**A3**	**A3**	**A3**		4 × 100 Mb - SC mm fiber
				A4	**A4**	**A4**	**A4**		8 × 10/100 Mb RJ45 copper
				A5	**A5**	**A5**	**A5**		2 × 10 Mb - ST mm fiber + 4 × 10/100 Mb RJ45 copper
				A6	**A6**	**A6**	**A6**		2 × 100 Mb - ST mm fiber + 4 × 10/100 Mb RJ45 copper
				A7	**A7**	**A7**	**A7**		2 × 100 Mb - SC mm fiber + 4 × 10/100 Mb RJ45 copper
				A8	**A8**	**A8**	**A8**		2 × 100 Mb - SC sm fiber 20 km + 4 × 10/100 Mb RJ45 copper
				AA	**AA**	**AA**	**AA**		4 × 100 Mb - LC mm fiber + 4 × 10/100 Mb - RJ45 copper
				AB	**AB**	**AB**	**AB**		8 × 100 Mb - LC mm fiber
				AC	**AC**	**AC**	**AC**		4 × 100 Mb - LC sm fiber + 4 × 10/100 Mb - RJ45 copper
				AD	**AD**	**AD**	**AD**		8 × 100 Mb - LC sm fiber
				AE	**AE**	**AE**	**AE**		2 × 100 Mb - LC sm fiber + 6 × 10/100 Mb - RJ45 copper
				AF	**AF**	**AF**	**AF**		2 × 10 Mb - ST mm fiber + 2 × 100 Mb - ST mm fiber
				AH	**AH**	**AH**	**AH**		8 x 100 Mb - MTRJ mm fiber
				AJ	**AJ**	**AJ**	**AJ**		4 x 100 Mb - MTRJ mm fiber + 4 x 10/100 Mb - RJ45 copper
				AK	**AK**	**AK**	**AK**		2 x 100 Mb - MTRJ mm fiber + 6 x 10/100 Mb - RJ45 copper
				G3	**G3**	**G3**	**G3**		1 × 1000 Mb - SC mm fiber 2 km + 2 x 100 Mb - SC mm fiber
				G4	**G4**	**G4**	**G4**		1 × 1000 Mb - SC mm fiber 2 km + 4 × 10/100 Mb - RJ45 copper
				G5	**G5**	**G5**	**G5**		2 × 1000 Mb - SC mm fiber 2 km
				G6	**G6**	**G6**	**G6**		1 × 1000 Mb - RJ45 copper
				G7	**G7**	**G7**	**G7**		1 × 1000 Mb - SC mm fiber 2 km
				G8	**G8**	**G8**	**G8**		1 × 1000 Mb - SC sm fiber 10 km
				GC	**GC**	**GC**	**GC**		1 × 1000 Mb - RJ45 copper + 2 × 100 Mb - SC mm fiber
				GD	**GD**	**GD**	**GD**		1 × 1000 Mb - RJ45 copper + 4 × 10/100 Mb - RJ45 copper
				GE	**GE**	**GE**	**GE**		2 × 1000 Mb - RJ45 copper
				GF	**GF**	**GF**	**GF**		1 × 1000 Mb - SC sm fiber 10 km + 2 × 100 Mb - SC mm fiber
				GH	**GH**	**GH**	**GH**		1 × 1000 Mb - SC sm fiber 10 km + 4 × 10/100 Mb - RJ45 copper
				GJ	**GJ**	**GJ**	**GJ**		2 × 1000 Mb - SC sm fiber 10 km
								X	Standard Environment
								H	Harsh Chemical Environment Option

1.3 Specifications

1.3.1 Technical Specifications

PERFORMANCE

Ethernet (10 Mb)..... 14880 pps
Fast Ethernet (100 Mb):..... 148,800 pps
Gigabit Ethernet (1000 Mb): ..... 1488000 pps
Switching processing: ..... Store and forward with IEEE 802.3x full-duplex flow - control, non-blocking
Data rate:..... 10 Mbps, 100 Mbps and 1000 Mbps
Address table capacity:..... 4K node, self-learning with address aging
Packet buffer size:..... 240 KB for 10/100; 120 KB for 1000 Mb
Latency: ..... 5 µs + packet time (100 to 100Mbps)
15 µs + packet time (10 to 10 Mbps and 10 to 100 Mbps)
RO mode recovery time (typical):..... ≤5 ms/hop

NETWORK STANDARDS AND COMPLIANCE

Ethernet V1.0/V2.0 IEEE 802.3: 10Base-T
IEEE 802.3u:..... 100Base-TX, 100Base-FX
IEEE 802.3z: ..... 1000Base-X Ethernet (auto-negotiation)
IEEE 802.3ab:..... 1000Base-X Ethernet
IEEE 802.1p:..... Priority protocol
IEEE 802.1d:..... Spanning tree protocol
IEEE 802.1q:..... VLAN tagging
IEEE 802.3x: ..... Flow control

MAXIMUM 10 MBPS ETHERNET SEGMENT LENGTHS

Unshielded twisted pair:..... 100 m (328 ft.)
Shielded twisted pair:..... 150 m (492 ft.)
10Base-FL multi-mode fiber optic: ..... 2 km (6562 ft.)
10Base-FL single-mode fiber optic: ..... 10 km (32810 ft.)

MAXIMUM STANDARD FAST ETHERNET SEGMENT LENGTHS

10Base-T (CAT 3, 4, 5 UTP): ..... 100 m (328 ft.)
100Base-TX (CAT 5 UTP):..... 100 m (328 ft.)
Shielded twisted pair:..... 150 m (492 ft.)
100Base-FX, half-duplex, multi-mode: 412 m (1350 ft.)
100Base-FX, full-duplex, multi-mode: .2.0 km (6562 ft.)
100Base-FX, half-duplex, single-mode: 412 m (1350 ft.)
100Base-FX, full-duplex, long reach: ...40.0 km (122K ft.)

MAXIMUM STANDARD GIGABIT ETHERNET SEGMENT LENGTHS

1000Base-T (CAT5e or higher is recommended): 100 m (328 ft.)
1000Base-SX, full-duplex, multi-mode (62.5 µm cable): 220 m
1000Base-SX, full-duplex, multi-mode (50 µm cable): 550 m

FIBER MULTI-MODE CONNECTORS

Fiber port, ST (twist-lock): ..... fiber multi-mode, 10 Mb 10Base-FL
Fiber port, SC-type (snap-in): ..... fiber multi-mode, 100Base-FX
Fiber port, ST-type (twist-lock): ..... fiber multi-mode, 100Base-FX
Fiber port, 1000Base-FX:..... GBIC modules

FIBER SINGLE-MODE CONNECTORS

Fiber port, SC-type: ..... Fiber optic single-mode, 100Base-FX
Fiber port, 1000Base-FX: ..... GBIC modules

LEDS

LK: ..... steady ON when media link is operational
ACT: ..... ON with receiver port activity
FDX/HDX: ..... ON = full-duplex mode
OFF = half-duplex mode
100/10: ..... ON = 100 Mbps; OFF = 10 Mbps

ALARM RELAY CONTACTS

One NC indicating internal power, one NC firmware controllable
Maximum Voltage: ..... up to 250 V AC, 220 V DC
Maximum Switching Power: ..... 60 W, 125 VA
Maximum Carrying Current: ..... 2 A @ 30 V DC
0.2 A @ 220 V DC

MANAGEMENT CONSOLE

Connector: ..... DB-9 for RS-232 "null-modem" cable (sometimes called an X-modem cable)

POWER SUPPLY

Input voltage: ..... LOW RANGE (LO Power Supply)
Nominal DC Voltage: 48 V DC
Min/Max DC Voltage: 36/60 V DC
..... HIGH RANGE (HI and AC Power Supply)
Nominal DC Voltage: 110 to 250 V DC
Min/Max DC Voltage: 88/300 V DC
Nominal AC Voltage: 100 to 240 V AC
Min/Max AC Voltage: 85/265 V AC
Input current (fiber): ..... LO: 1.59 A maximum
HI: 1.8 A maximum for AC voltage
0.9 A maximum for DC voltage
AC: 1.8 A maximum
Standard terminal block: ..... "–", "+", internally floating
Ground: ..... Terminal for filter ground wire, external connection to the ML2400 chassis
Power consumption: ..... 55 watts typical; 60 watts maximum for a fully loaded fiber model; 35 watts maximum for a fully-loaded RJ45 model
Internal Fuse: ..... **HI**: Ceramic, axial SLO BLO, 3 A /350 V AC
Manufacturer: Conquer
Part Number: SCD-A 003
LO: Ceramic, axial SLO BLO, 5 A /350 V AC
Manufacturer: Conquer
Part Number: SCD-A 005

PER-PORT JUMPERS AND SWITCHES

The copper daughter board has on internal switch for selecting MDI-MDIX crossover on port # 1. Other port-specific user settings (such as FDX or HDX, copper 10/100 speed) can be fixed using firmware commands.

1.3.2 Environmental Specifications

OPERATING ENVIRONMENT

Ambient temperature: .....–40 to 185°F (–40 to 85°C) for IEC 60068-2-1, IEC 60068-2-2 for 16 hours
Nominal ≤ 50°C
Storage temperature:.....–60 to 210°F (–50 to 100°C)
Ambient relative humidity: .....5% to 95% (non-condensing)
Altitude:.....2000 m

1.3.3 Type Tests

Standard Name	Standard Number:Date code	Severity levels Tested
Electrostatic Discharge: Air and Direct	EN/IEC61000-4-2:1995	8Kv contact,15Kv Air (Level 4)
Electrostatic Discharge: Air and Direct	IEEE C37.90.3:2001	8Kvcontact,15Kv air
Electrical Fast Transient/ Burst Immunity	EN/IEC61000-4-4:2004	(+/-4KV @2.5Khz for Common and Transverse modes) & 2KV 5Khz Common and transverse (Level 3 & 4)
Electrical Fast Transient/ Burst Immunity	IEEE C37.90.1:2002	Class 4 (+/-4KV for Common and Transverse modes)
Power Transients)high repetition	NEMA TS2 2.1.6.1:2003	300V,2500W
Power Transients (low repetition high energy)	NEMA TS2 :2003	600V, 1 ohm impedance
Transients I/O terminals	NEMA TS2 2.1.7.1 :2003	300V,1000ohms impedance
Surge Immunity	IEC61000-4-5:2005	Class 4 (2KV Line to Earth and 1KV Line to Line) Installation Class 3, Level 2 & 3
Non Destructive transient Immunity	NEMA TS2:2003	1000V,1 ohm X 3
Ring Wave Surge ,IEC Damped Oscillatory Burst 1Mhz	EN/IEC61000-4-12 :2006	Ring wave: (1KV Common), 0.5KV (diff) (Level 2)
SWC Damped Oscillatory	IEEEC37.90.1:2002	Common and transverse to 2.5KV, No Transverse for Data Comms and Signal cct
Voltage Dip; 2. Voltage Interruption;	EN/IEC 61000-4-11 :2004	0%(5000msec),40%(6 cycles), 70%(10msec) of test voltage
Ripple on DC power I/P port	IEC 61000-4-17	10% of rated voltage (Level 3)
RF Immunity 80-1000MHz	EN/IEC 61000-4-3 :1998	10V/m (Level 3)
RF Immunity 80-1000MHz	IEEE C37.90.2:2004	35V/m (20V/m + modulation)
Conducted RF Immunity 150Khz -80 MHz	IEC61000-4-6:1996	10Vrms (Level 3)
Conducted RF Immunity 0-150Khz	EN/IEC 61000-4-16:1998	15Hz-150 Khz 1-10V (Level 3)
Power Frequency Magnetic Field Immunity	EN/IEC 61000-4-8:1993,2001	continuous 100/200A/m (Level 5 - continuous)
Damped magnetic Immunity	IEC61000-4-10	10A/m (Level 3)
Voltage dips and Interrupts for DC power ports	IEC61000-4-29	All test levels and durations - Passes to Criteria B
Conducted & Radiated Emissions	CISPR22 / EN 55022	Class A
Conducted & Radiated Emissions	FCC Part 15 Subpart B	Class A

Standard Name	Standard Number:Date code	Severity levels Tested
A-rated control power inputs	IEEE 1613:2003	Test operation @85% to110% or rated - as per 5.1 and 5.3
AC voltage ranges	IEC60870-2-1	+ / - 10% (AC1)
DC voltage ranges	IEC60870-2-1	+ / - 15% (DC2)
ENVIRONMENTAL TESTS		
Relative Humidity Cyclic	EN/IEC 60068-2-30:2005	6-day 93% @ 55deg C (Variant 2)
Cold Temperature	EN/IEC 60068-2-1: 1993/1990	16 hours -40 deg start up (Ad)
Dry Heat Temperature	EN/IEC 60068-2-2:1994,1974	16 hours at rated upper limit, hot start up (Bd)
Humidity: -34 to 74C, 10-95%	NEMA TS2	Humidity: -34 to 74C, 10-95% Defined in 2.1.5
MECHANICAL TESTS		
Sinusoidal Vibration	EN/IEC 60255-21-1 :1996,1988,	10-150hz Response/Endurance @1G (Class 1)
Shock; 2. Bump;	EN/IEC 60255-21-2:1996,1988	Class 2 for shock(30g) and Bump (20g) (Class 2)
Shock	NEMA TS2	10g, x,,y,z (As per 2.2.9)
Vibration Endurance	NEMA TS2	Vibration 5-30Hz 0.015" research+ 1hr(0.5g) dwell on resonant freq (As per 2.2.8)
Vibration	MIL-STD -167-1 (variable amplitudes 4-50Hz)	5-30Hz,0.5g plus resonance frequency dwell (Type 1 Environmental vibration)
FUNCTIONAL TESTS		
Operating Voltage	NEMA TS2 -89-135VAC	Test @max nominal rating (As per 2.1.2)
Operational frequency	NEMA TS2 -57-63Hz	60Hz +/- 3Hz (As per 2.1.3)
SAFETY TESTS		
IT -Safety	EN60950-1:2006	
UL IT -Safety	UL60950-1	
cUL IT -Safety	C22.2 No. 60950-1	
Dielectric	IEEE 1613:2003	2000V (2000VAC & 500VAC)
Impulse	IEEE 1613:2003	5000V

1.3.4 Physical Specifications

MOUNTING

Vertical: ..... suitable for stand-alone or rack mounting

PACKAGING

Enclosure: ..... rugged high-strength sheet metal

Dimensions: ..... 1.70 in. × 17.0 in. × 9.2 in. (H × W × D)
4.32 cm × 43.2 cm × 22.9 cm (H × W × D)

1.3.5 Approvals and Warranty

APPROVALS

FCC: ..... Emissions meet FCC part 15 class A

NEBS: ..... level 3

ETSI: ..... certified for carrier central offices

IEEE: ..... IEEE P1613 environmental standard for electric power substations

IEC:.....IEC61850 EMC and operating conditions class C for power susbstations
CE:.....EN 50082-1, EN 55022:1998, EN 60950 3rd Edition
UL:.....UL listed/recognized (file E156407), UL 60950-1 1st edition
CSA:.....Certified per C22.1 No. 60950-1 1st edition

WARRANTY
24 months from date of shipment
Manufactured in USA
GE Multilin reserves the right to change specifications, performance, characteristics, and/or model offerings without notice.

1.4 Firmware Overview

1.4.1 Command Line Firmware

Commands typed by the user will be shown in the following color and font.

```
command
```

The MultiLink Switch Software prompt will be shown in bold and fixed-width text, with a **#** or **>** character at the end. The default prompt is indicated as follows:

ML2400#

The following hold for syntax rules:

- Syntax rules are italicized
- The command part is in bold
- Optional entries are shown in [square brackets]
- Parameter values within are shown in <pointed brackets>
- Optional parameter values are shown again in [square brackets]

Thus, the syntax

command *[parameter1=<value1>[,paramter2=<value2>]] parameter3=<value3|value4>*

indicates the following:

- parameters 1 and 2 are optional
- parameter 2 can be used optionally only if parameter 1 is specified
- parameter 3 is mandatory.

Whenever the word PC is used, it implies a UNIX, Linux, Windows, or any other operating system based workstation, computer, personal computer, laptop, notebook or any other computing device. Most of the manual uses Windows XP based examples. While effort has been made to indicate other operating system interactions, it is best to use a Windows-XP based machine when in doubt.

The documentation reflects features of MultiLink Switch Software version 1.7.x or later. If your switch is not at the current version, GE Multilin recommends upgrade to version 1.7.x or later. Please refer to the GE Multilin website for information on upgrading the MultiLink Switch Software.

1.4.2 EnerVista Software

Icons common to the EnerVista MultiLink Secure Web Management (SWM) firmware for edit, delete, save and refresh are:

- Edit - edit the values
- Delete - delete the current row or the value(s)
- Save - save configuration changes
- Refresh - repaint the screen

1.4.3 Before Starting

This section explains how to setup the GE MultiLink family of switches using the console port on the switch. Some of the functionality includes setting up the IP address of the switch, securing the switch with a user name and password, setting up VLANs and more.

Before you start, it is recommended to acquire the hardware listed below and be ready with the items listed.

For initial configuration through the serial/console port:

1. A female-female null modem cable.
2. A serial port. If your PC does not have a serial port, you may want to invest in a USB-to-serial converter or USB-to-serial cable.
3. Terminal emulation firmware such as HyperTerminal or other equivalent firmware. Ensure the firmware supports Xmodem protocol, as you may need this in the future to update the MultiLink Switch Software.
4. Enough disk space to store and retrieve the configuration files as well as copy firmware files. We recommend at least 15 MB of disk space for this purpose.
5. For access security - decide on a manager level account name and password
6. IP address, netmask, default gateway for the switch being configured.

As a default, the switch has no IP (Internet Protocol) address and subnet mask. For first time use, the IP address has to be assigned. This can only be done by using the console interface provided.

The same procedure can also be used for other configuration changes or updates (for example, changing the IP address, VLAN assignments and more). Once the IP address is assigned and a PC is networked to the switch, the switch's command line interface (CLI) can be accessed via telnet. To manage the switch through in-band (networked) access (e.g. telnet, or web browser Interface), you should configure the switch with an IP address and subnet mask compatible with your network. Also, change the manager password to control access privileges from the console.

Many other features such as optimizing the switch's performance, traffic engineering and traffic prioritizing, VLAN configuration, and improving network security can be configured through the switch's console interface as well as in-band (networked) access, once the IP address is setup. Besides the IP address, setting up the SNMP parameters allows configuration and monitoring through an SNMP network management station running a network management program.

1.5 Command Line Interface Firmware

1.5.1 Console Connection

The connection to the console is accessed through the DB-9 RS232 connector on the switch marked as the console port. This command line interface (or CLI) provides access to the switch commands. It can be accessed by attaching a VT100 compatible terminal or a PC running terminal emulation firmware to the console port.

USB-to-serial adapters are also available for computers that do not native serial ports but have access to USB ports.

The interface through the console or the console management interface (or CMI) enables you to reconfigure the switch and to monitor switch status and performance.

Once the switch is configured with an IP address, the command line interface (or CLI) is also accessible using telnet as well as the serial port. Access to the switch can be either through the console interface or remotely over the network. Simultaneous access (that is, through the console port as well as through the network) to the MultiLink switch is not permitted.

The Command Line Interface (CLI) enables local or remote unit installation and maintenance. The MultiLink family of switches provides a set of system commands which allow effective monitoring, configuration and debugging of the devices on the network.

1.5.2 Console Setup

Connect the console port on the switch to the serial port on the computer using the serial cable listed above. The settings for the HyperTerminal firmware emulating a VT100 are shown below. Make sure the serial parameters are set as shown (or bps = 38400, data bits = 8, parity = none, stop bits = 1, flow control = none).

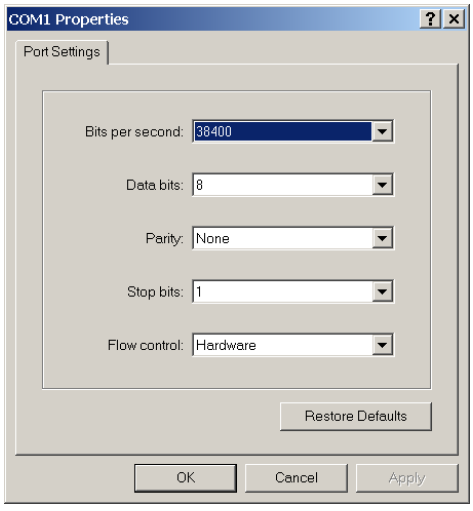


FIGURE 1–1: Serial Settings in HyperTerminal

1.5.3 Console Screen

Once the console cable is connected to the PC and the firmware configured, ML2400 legal disclaimers and other text scrolls by on the screen.

The line interface prompt appears displaying the switch model number (e.g. **ML2400>**)

The switch has three modes of operation: *operator* (least privilege), *manager*, and *configuration*. The prompts for the switches change as the switch changes modes from operator to manager to configuration. The prompts are shown below with a brief description.

- **ML2400>**
  Operator Level - for running operations queries
- **ML2400#**
  Manager Level - for setting and reviewing commands
- **ML2400##**
  Configuration Level - for changing the switch parameter values

For additional information on default users, user levels and more, refer to *User Management* on page 1–14.

1.5.4 Logging In for the First Time

For the first time, use the default user name and passwords assigned by GE. They are:

- Username: **manager**
  Password: **manager**
- Username: **operator**
  Password: **operator**

We recommend you login as manager for the first time to set up the IP address as well as change user passwords or create new users.

1.5.5 Automatic IP Address Configuration

The ML2400 is operational immediately after it is powered up. The advanced management and configuration capabilities of the ML2400 allows you to easily configure, manage, and secure your devices and network.

Before starting, ensure you have the following items:

- RJ45 Ethernet cable
- PC with an Ethernet port
- Microsoft Internet Explorer 6.0 or higher
- Macromedia Flash Player 5.0 or higher (available from http://www.macromedia.com/shockwave/download/download.cgi?P1_Prod_Version=ShockwaveFlash)

Ensure both firmware components are installed before proceeding.

The ML2400 can search the network for commonly used services that can issue an IP address. If the switch is connected to a network, the ML2400 uses the following process to find an IP address.

NOTE

If the ML2400 is not connected to a network, then proceed to Step 3 below. or use the default IP address.

Step 1:

The ML2400 will scan the network for a DHCP server. If the server responds, the ML2400 will acquire and set the assigned IP address. To manage the switch, determine the assigned IP address and enter as follows in Internet Explorer:

https://<*assigned_IP_address*>

Ensure that **https** is entered, not **http**, and that there is connectivity (that is, you can ping the switch).

Step 2:

If there is no response from a DCHP server, the ML2400 will query for a BOOTP server. If the server responds, the ML2400 will acquire and set the assigned IP address. To manage the switch, determine the assigned IP address and enter as follows in Internet Explorer:

https://<*assigned_IP_address*>

Ensure that **https** is entered, not **http**, and that there is connectivity (that is, you can ping the switch).

Step 3:

If there is no response from either a DCHP or BOOTP server, or if the switch is not connected to a network, the switch will assign itself an IP address. The ML2400 will check to see if IP address **192.168.1.2**, with a network mask of 255.255.255.0, is free. If so, it will assume these values. If this IP address is assigned to another device, the ML2400 will repeat steps 1 through 3 to find a DCHP or BOOTP server or wait for the **192.168.1.2** address to become free.

Once connected, the browser will display a login prompt. The default login is:

- Username: **manager**
  Password: **manager**

1.5.6 Setting the IP Parameters

To setup the switch, the IP address and other relevant TCP/IP parameters have to be specified.

The IP address on the MultiLink switch is set to **192.168.1.2** from the factory. The switch is fully operational as a Layer 2 switch as a default. Setting a default IP address can potentially cause duplicate IP address problem if multiple switches are powered on and installed on the network. To manage the switch, an IP address has to be programmed.

Before starting, please ensure that the IP address assigned to the switch is known or contact your system/network administrator to get the IP address information. Follow the steps listed below to configure the switch.

- ▷ **Ensure the power is off.**
- ▷ **Follow the steps described above for connecting the console cable and setting the console firmware.**
- ▷ **Power on the switch.**

- Once the login prompt appears, login as manager using default password (manager).
- Configure the IP address, network mask and default gateway as per the IP addressing scheme for your network.
- Set the manager password (this step is recommended; refer to the following section).
- Save the settings (without saving, the changes made will be lost).
- Power off the switch (or a firmware reboot as discussed below).
- Power on the switch - login with the new login name and password.
- From the PC (or from the switch) ping the IP address specified for the switch to ensure connectivity.
- From the switch ping the default gateway specified (ensure you are connected to the network to check for connectivity) to ensure network connectivity.

Syntax:

ipconfig *[ip=<ip-address>] [mask=<subnet-mask>] [dgw=<gateway>]*

An example is shown below.

```
ML2400# ipconfig ip=3.94.247.41 mask=255.255.252.0
dgw=3.94.247.41
ML2400# save
```

This manual assumes the reader is familiar with IP addressing schemes as well as how net mask is used and how default gateways and routers are used in a network.

Reboot gives an opportunity to save the configuration prior to shutdown. For a reboot, simply type in the command `reboot`. Note that even though the passwords are not changed, they can be changed later.

```
ML2400# reboot
Proceed on rebooting the switch? ['Y' or 'N'] Y
Do you wish to save current configuration? ['Y' or 'N'] Y
ML2400#
```

The ML2400 forces an answer by prompting with a "Y" or a "N" to prevent accidental keystroke errors and loss of work.

The parameters can be viewed at any time by using the `show` command. The show command will be covered in more detail later in various sections throughout the document.

The example below illustrates the basic setup parameters. You can use `show setup` or `show sysconfig` commands to view setup parameters.

```
ML2400# show setup
Version: ML2400 build 1.6.1 Apr 29 2005 11:10:13
MAC Address:  00:20:06:27:0a:e0
IP Address: 3.94.247.41
Subnet Mask: 255.255.252.0
Gateway Address: 3.94.244.1
CLI Mode: Manager
System Name: ML2400
```

```
System Description: 25 Port Modular Ethernet Switch
System Contact: multilin.tech@ge.com
System Location: Markham, Ontario
System ObjectId: 1.3.6.1.4.1.13248.12.7
```

ML2400# `show sysconfig`

```
System Name: ML2400
System Contact: multilin.tech@ge.com
System Location: Markham, Ontario
Boot Mode:  manual
Inactivity Timeout(min): 120
Address Age Interval(min): 300
Inbound Telnet Enabled: Yes
Web Agent Enabled: Yes
Time Zone: GMT-05hours:00minutes
Day Light Time Rule: Canada
System UpTime: 0 Days 0 Hours 45 Mins 55 Secs
```

ML2400#

Some of the parameters in the MultiLink family of switches are shown above. The list of parameters below indicates some of the key parameters on the switch and the recommendations for changing them (or optionally keeping them the same).

1.5.7 Privilege Levels

Two privilege levels are available - manager and operator. Operator is at privilege level 1 and the manager is at privilege level 2 (the privilege increases with the levels). For example, to set up a user for basic monitoring capabilities use lower number or operator level privilege (level 1).

The Manager level provides all operator level privileges plus the ability to perform system-level actions and configuration commands. To select this level, enter the `enable <user-name>` command at the Operator level prompt and enter the Manager password, when prompted.

enable *<user-name>*

For example, switching from an operator-level to manager-level, using the `enable` command is shown below.

ML2400> `enable manager`

```
Password: *******
```

ML2400#

Note the prompt changes with the new privilege level.

Operator privileges allow views of the current configurations but do not allow changes to the configuration. A ">" character delimits the operator-level prompt.

Manager privileges allow configuration changes. The changes can be done at the manager prompt or for global configuration as well as specific configuration. A "#" character delimits any manager prompt.

1.5.8 User Management

A maximum of five users can be added per switch. Users can be added, deleted or changed from a manager level account. There can be more than one manager account, subject to the maximum number of users on the switch being restricted to five.

To add a user, use the `add` command as shown below. The user name has to be a unique name. The password is recommended to be at least 8 characters long with a mix of upper case, lower case, numbers and special characters.

add *user=<name> level=<number>*

The following example adds a user "peter" with manager-level privilege:

```
ML2400# user
ML2400(user)## add user=peter level=2
Enter User Password:******
Confirm New Password:******
ML2400(user)##
```

To delete a user, use the `delete` command as shown below.

delete *user=<name>*

The following example deletes the user "peter":

```
ML2400(user)## delete user=peter
Confirm User Deletion(Y/N): Y
User successfully deleted
ML2400(user)##
```

The syntax to modify a password is shown below:

passwd *user=<name>*

The following example changes the password for user "peter".

```
ML2400(user)## passwd user=peter
Enter New Password:******
Confirm New Password :******
Password has been modified successfully
ML2400(user)##
```

The syntax to modify the privilege level for a specific user is shown below:

chlevel user=<name> level=<number>

The following example modifies the privilege level of user "peter" to Operator privileges.

```
ML2400(user)## chlevel user=peter level=1
Access Permission Modified
ML2400(user)##
```

The syntax to set the access privileges for telnet and Web services is shown below:

useraccess *user=<name> service=<telnet|web> <enable|disable>*

The following example sets the access privileges for telnet and Web services.

```
ML2400(user)## useraccess user=peter service=telnet disable
Telnet Access Disabled.
```

1.5.9 Help

Typing the `help` command lists the commands you can execute at the current privilege level. For example, typing `help` at the Operator level shows the following:

```
ML2400> help
```

```
logout      ping        set
terminal    telnet      walkmib

Contextless Commands:

!           ?           clear
enable      exit        help
show        whoami
alarm
```

ML2400>

Help for any command that is available at the current context level can be viewed by typing help followed by enough of the command string to identify the command. The following syntax applies:

help *<command string>*

For example, to list the help for the `set time` command

ML2400# `help set time`

```
set time    : Sets the device Time

Usage

set time hour=<0-23> min=<0-59> sec=<0-59> [zone=GMT[+/-]hh:mm]
```

ML2400#

The options for a specific command can be displayed by typing the command and pressing enter. The following syntax applies:

command *<Enter>*

For example, the options for the `show` command are:

ML2400# `show <Enter>`

```
Usage

  show active-stp
  show active-snmp
  show active-vlan
  show address-table
  show age
  show alarm
  show arp
  show auth <config|ports>
  show backpressure
  show bootmode
  --more--
```

Other ways to display help, specifically, with reference to a command or a set of commands, use the TAB key. The following syntax applies:

<TAB>

<Command string> <TAB>

<First character of the command> <TAB>

For example, following the syntax listed above, the <TAB> key will list the available commands in the particular privilege level:

ML2400> `<TAB>`

```
  ?
  alarm
  clear
  enable
  exit
  help
  logout
```

```
ping
set
show
telnet
terminal
walkmib
whoami
```

ML2400>

The following example lists commands starting with a specific string:

ML2400> s <TAB>

```
set
show
```

ML2400>

In the following example, the <TAB> key completes the command:

ML2400> se<TAB>

```
password
timeout
vlan
```

ML2400> set

1.5.10 Exiting

To exit from the CLI interface and terminate the console session use the `logout` command. This command prompts to ensure that the logout was not mistakenly typed. The following syntax applies:

logout

The following example illustrates logging out from a session:

ML2400> logout

```
Logging out from the current session ['Y' or 'N'] Y
Connection to the host lost
```

1.6 EnerVista Secure Web Management

1.6.1 Logging in for the First Time

Enter the following URL in the web browser to login to the EnerVista Secure Web Management software.

```
https://<IP Address assigned to the switch>
```

NOTE

Make sure you use HTTPS (secure HTTP) and not HTTP in the URL.

In the example shown in the previous section, the URL is:

```
https://3.94.247.41
```

If your site uses name services, you can use a name instead of the IP address. Please make sure that the name is resolved to the IP address assigned to the switch.

The secure site will issue the certificate check shown below.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

FIGURE 1–2: Security certificate

Once you click **Yes** on the security certificate, the browser will prompt you to login.

FIGURE 1–3: Login screen

For the first time,

▷ Login with the name **manager** and password **manager**.

▷ Click on **Login**.

After a successful login, the welcome screen is shown. Note the different information provided on the screen and different areas. The menus are used to configure settings on the switch. Users can click on a specific port to open the port configuration view.

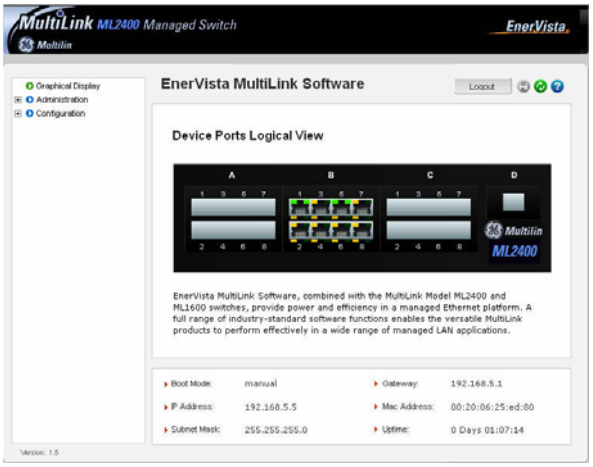


FIGURE 1–4: Welcome screen

1.6.2 Privilege Levels

- **Operator privilege users**: operator privileges allow views of the current configurations but do not allow changes to the configuration.
- **Manager privilege users**: manager privileges allow configuration changes. The changes can be done at the manager prompt or for global configuration as well as specific configuration.

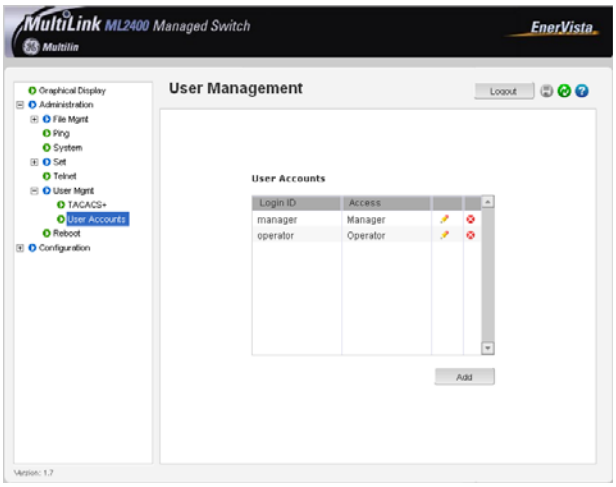
1.6.3 User Management

A maximum of five users can be added per switch. Users can be added, deleted or changed from a manager level account. There can be more than one manager account, subject to the maximum number of users on the switch being restricted to five.

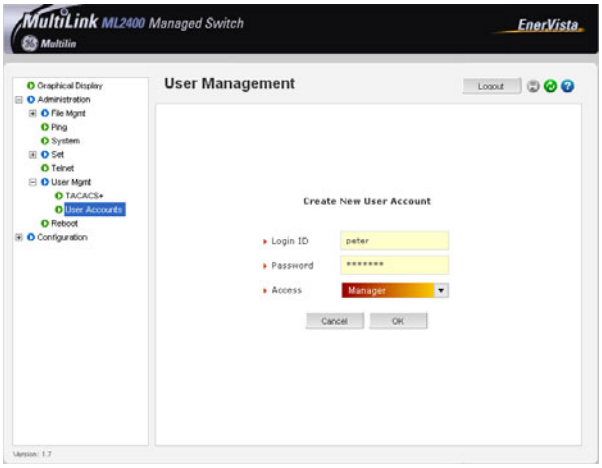
▷ Select the **Administration > User Mgmt > User Accounts** menu item.

▷ To add a user, use the **add** button.

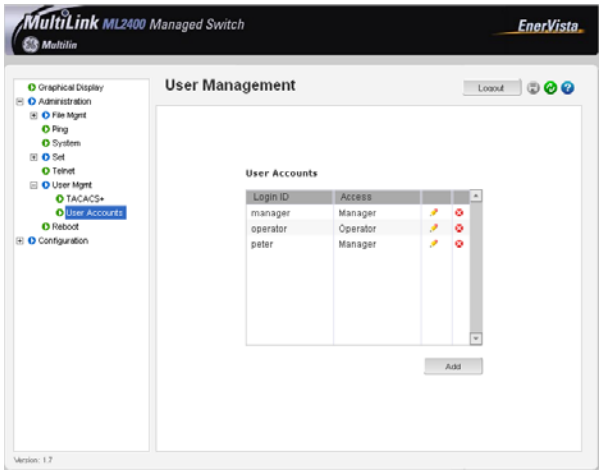
The username must be a unique name. The password is recommended to be at least 8 characters long with a mix of upper case, lower case, numbers and special characters.



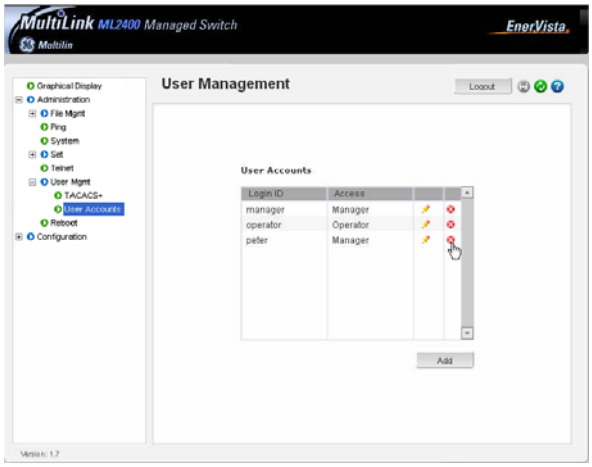
In the following example below, the user **peter** was added with manager privilege after clicking the **add** button.



After successfully adding a user, the added user is displayed in the list of users as shown below.

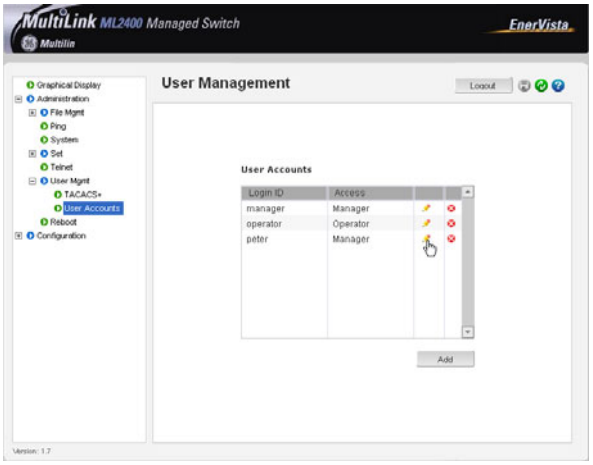


▷ To delete a user, click on the delete icon ( ) as shown below.

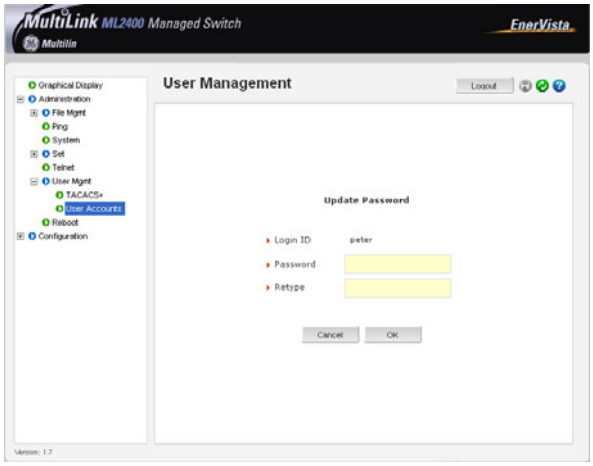


The firmware will prompt to verify the delete command.

▷ To modify the password, view the users as described above and click on the edit icon ( ).



After clicking on the **edit** icon, the screen opens up for modifying the password.



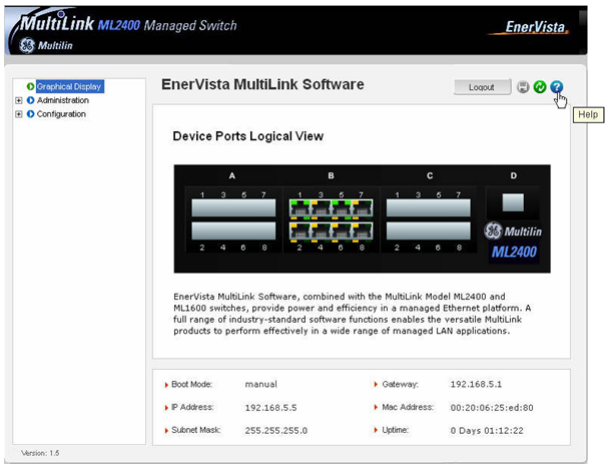
In this example, the user ID **peter** was selected for modification. The password for **peter** will be modified after the new password is entered.

1.6.4 Modifying the Privilege Level

Privilege levels cannot be changed from the EnerVista Secure Web Management (SWM) firmware. This can only be done through the CLI interface, or alternately, by deleting the user and adding the same user with the proper privilege level.

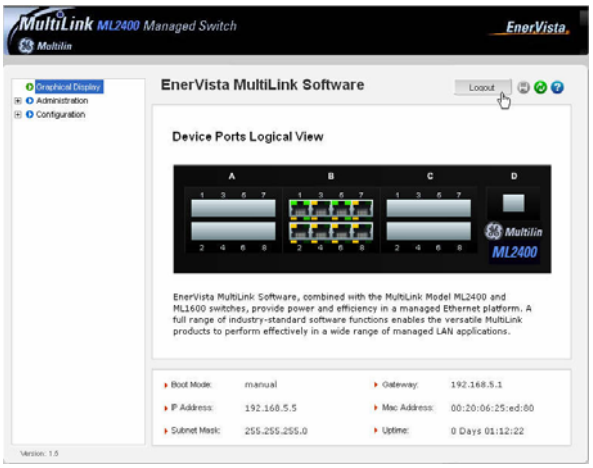
1.6.5 Help

Help for the EnerVista Secure Web Management software can be obtained by clicking on the Help icon as shown below.



1.6.6 Exiting

▷ To exit or logout, click on the **logout** button.


MultiLink ML2400 Managed Switch
EnerVista
Graphical Display
Administration
Configuration
EnerVista MultiLink Software
Logout
Device Ports Logical View
A
B
C
D
Multilin
ML2400
EnerVista MultiLink Software, combined with the MultiLink Model ML2400 and ML1600 switches, provide power and efficiency in a managed Ethernet platform. A full range of industry-standard software functions enables the versatile MultiLink products to perform effectively in a wide range of managed LAN applications.
Boot Mode: manual
Gateway: 192.168.5.1
IP Address: 192.168.5.5
Mac Address: 00:20:06:25:ed:80
Subnet Mask: 255.255.255.0
Uptime: 0 Days 01:12:22

▷ Confirm the logout by selecting OK in the pop-up window.

1.7 ML2400 Firmware Updates

1.7.1 Updating MultiLink Firmware

This section describes how to upgrade the firmware on a Multilink switch, either locally at the console port or remotely over the network using FTP or TFTP. Depending on the update process (serial/console port or network), ensure the necessary tools listed below are available, tested and working before you begin.

For serial port updates directly through the serial/console port, the following items are required.

1. A female-to-female null modem cable.
2. A USB-to-serial converter or cable if your PC does not have a serial port. A cable is available from GE Multilin.
3. Terminal emulation firmware such as HyperTerminal (included with Windows) or equivalent. Ensure that the firmware supports the Xmodem protocol
4. At least 15 MB of free disk space.
5. Manager level account name and password of the switch being upgraded.
6. An internet connection. Ensure the connection does not block ftp file transfers

1.7.2 Selecting the Proper Version

Ensure that the proper version of the MultiLink Switch Software is installed. The latest version of the firmware is available at http://www.GEmultilin.com.

- ▷ **Connect to the ML2400 and login as manager.**
- ▷ **Enter the `show version` command.**
- ▷ **Download the latest version of MultiLink firmware from the GE Multilin website.**

1.7.3 Updating through the Command Line

Use the following procedure to install firmware to the ML2400 via the serial port.

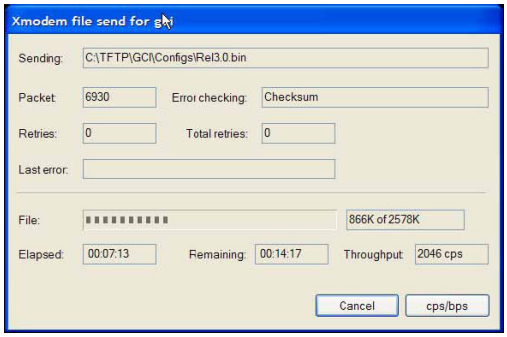
- ▷ **Download the MultiLink Switch Software from the GE Multilin web site.**
- ▷ **Use the null-modem cable to connect to the ML2400 serial port.**
- ▷ **Login at the manager level with the proper password.**
- ▷ **Save the existing configuration (refer to *Saving Configuration* on page 5–19 for details).**
- ▷ **Enter the following command:**

```
ML2400# xmodem get type=app
Do you wish to upgrade the image? [Y or N] Y
Please start XModem file transfer now.
```

Refer to *Saving Configuration* on page 5–19 for details on the `xmodem` command.

Once the upgrade is started, the terminal emulation firmware will ask for the installation file location.

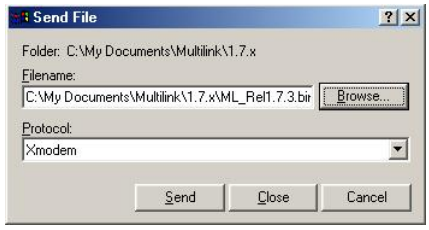
- ▷ Indicate the file location to begin the file transfer.
- ▷ Make sure the Xmodem protocol is also selected in this file location dialog window.



In some operating systems it maybe necessary to select the transfer option.

In this case,

- ▷ Return to the HyperTerminal window used in step 5.
- ▷ Select the **Transfer > Send File** menu item.
- ▷ As shown below, enter the location of the new firmware file.
- ▷ Select the Xmodem protocol.



- ▷ Select the **Send** button and to begin the file transfer.
- ▷ Once the file transfer is completed reboot the switch with the `reboot` command or by cycling power.
- ▷ Login to the switch and use the `show version` command to verify and upload the configuration file (if necessary).

1.7.4 Updating through the enervista Software

Use the following procedure to install the EnerVista Secure Web Management software.

- ▷ Download the latest MultiLink firmware from the GE Multilin web site.
- ▷ Save this file on FTP or TFTP. Ensure the FTP or TFTP path is configured. If using FTP, record the FTP login name and password.

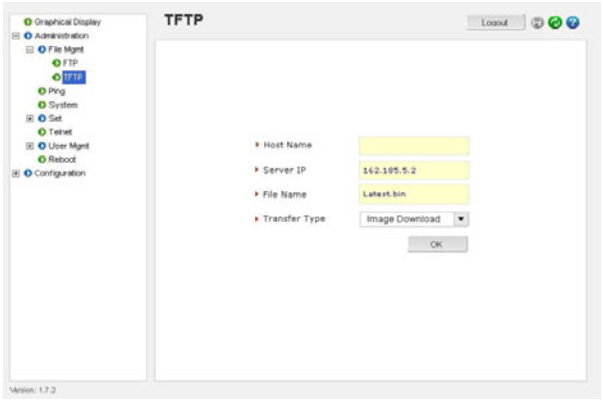
▷ **Select the switch to upgrade. Ensure you have system administration privileges available on the switch.**

▷ **Open a EnerVista Secure Web Management software session with the switch by typing in the following URL:**

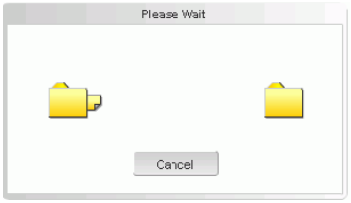
https://<IP address of the switch>

If using FTP, save the configuration before proceeding. GE Multilin recommends a two-step update: first save the configuration to the ftp server, then load the new image and restart the switch (refer to *Saving Configuration* on page 5–19 for details on saving the configuration).

▷ **Load the new firmware as shown below.**



As the file is being loaded, the firmware will display the transfer in progress window.

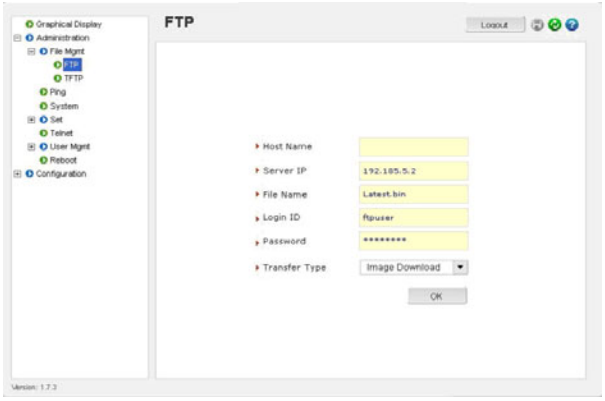


▷ **Reboot the switch when the transfer is complete. After reboot, the firmware is ready for use.**

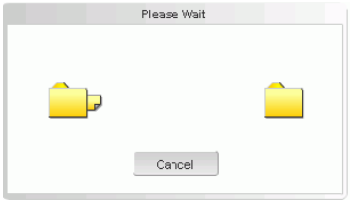
▷ **If using TFTP, save the configuration before proceeding. GE Multilin recommends a two-step update:**

- first save the configuration to the TFTP server,
- then load the new image and restart the switch (refer to *Saving Configuration* on page 5–19 for details on saving the configuration).

▷ **Load the new firmware as shown below.**



As the file is being loaded, the firmware will display the transfer in progress window.



▷ **Reboot the switch when the transfer is complete.**

After reboot, the firmware is ready for use.

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 2: Product Description

2.1 Overview

2.1.1 Introduction to the ML2400

The MultiLink ML2400 Ethernet Switch boosts the performance of large Ethernet LANs, typically serving as a “backbone” switch. It has the flexibility to handle a mix of both fiber and twisted-pair switched ports along with Gigabit backbone port options. Industry-standard IEEE 802.1p QoS prioritization is included, providing high performance switching services for both “smooth” streaming and “bursty” data traffic.

The MultiLink ML2400 Ethernet Switch has up to 25 ports capacity, all of which may be configured as fiber ports, while offering a space-saving rack-mount chassis that is only 1 U (1.70 inches or 4.32 cm) in height. The “mixed-media” capability allows user-selection of all popular flavors of fiber port connectors and modes, including 10Mb fiber alongside Gigabit ports. It also allows a mix of 10/100Mb RJ45 (copper) ports and a fiber Gigabit port in the same unit. This flexibility is achieved via a family of communication modules for copper and fiber, six-port modules for fiber and RJ45 combinations, and 1 Gb port module selections using GBICs. These modules are factory configured in a base chassis unit (or may be changed in the field by trained technicians) to adapt the unit to the user's application and Ethernet cabling requirements. Evolving mixed-media requirements for 10 Mb and 100 Mb fiber and copper as well as Gigabit ports can be handled by the ML2400.

The packaging and power-input options target the ML2400 at heavy-duty applications. Rack widths accommodated include standard 19" RETMA, ETSI, and 23". Input power may be 48 V DC for telecommunications environments or 125 V DC for industrial applications. Redundant power supplies are optional on all models.

2.1.2 Design Aspects

Designed for use in network traffic centers, the MultiLink ML2400 Ethernet Switch is easy to install and use. Addresses of attached nodes are automatically learned, maintained, and aged out, adapting the switching services to network changes. LEDs provide status information on each port. The ML2400 provides high performance plug-and-play hardware operation, 802.1p packet prioritization in hardware, and industry-standard managed networks software functionality, all in convenient 1 U rack-mount packages.

The ML2400 is a 19" rack-mountable Ethernet switch with three eight-port slots (A, B, and C) and one Gb-only slot (D). Slots A, B and C may be configured with a selection of fiber and copper ports. Slot D may be configured with a Gb module that accepts GBICs. These configurable ports allow the ML2400 to efficiently serve a large variety of applications. The ML2400 modules are usually factory installed, but may be changed or added at a later date in the field.

Status LEDs are part of each port module and are viewable when connecting the Ethernet media. The port status data is also accessible through the MultiLink Switch Software.

2.2 Communications Modules

2.2.1 Four-Port Modules

The four-port fiber option for the modular slot comes in three configurations:

- A1 module: 4 × 10 Mb – ST mm fiber
- A2 module: 4 × 100 Mb – ST mm fiber
- A3 module: 4 × 100 Mb – SC mm fiber

FIGURE 2–1: Example two-Port 10Mb mm fiber ST module & two-Port 100Mb mm fiber ST module

The default setup on the 10 Mb fiber module is half-duplex, which allows the ML2400 to connect to any 10 Mb hub, media converter, or almost any device with a 10 Mb fiber Ethernet port. The default setting of the 100 Mb fiber modules is full-duplex. User mode control per port through the software “port settings” is the same as the other modules.

NOTE

The status LED layout on a 10Mb fiber port pair is different from that on a 100 Mb fiber port pair. Notice that on the above image, where the 2 x 10 Mb ST mm fiber poarts have three LEDs next to each port, the 2 x 100 Mb ST mm fiber ports have 4 LEDs combined for the 2 ports, and under each port is a link LED. In both cases, the number of status LEDs is the same for each port.

There are three LEDs per fiber port. The Link (LK) LED, when lit, indicates "ready for operation" on that port, the F/H LED indicates operation in full-duplex mode when ON (half-duplex when OFF), and the blinking ACT LED indicates receiving activity on the port. A fiber cable must be connected to the port, and the link (LK) indicator for that port must be ON (indicating there is a powered-up device at the other end of the cable) in order for a LK LED to provide valid indications of operating conditions on that port. Color-coding on the panel of the module shows which LEDs belong to which port.

The fiber ports support fiber cabling distances according to the 10Base-FL and 100Base-FX standards, i.e., 2 km distance for multi-mode fiber. A single-mode option for greater distance may be available as a special order, contact GE Multilin.

The combo four-port modules are combinations of copper and fiber media, available as two 10/100 switched RJ45 copper ports and two 100 Mb switched multi-mode fiber ST or SC ports as shown below.

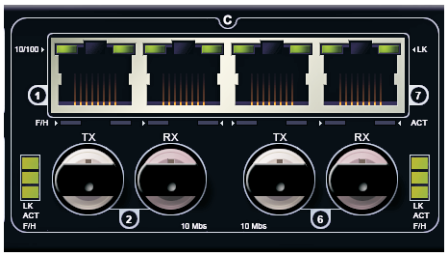
- AF module: 2 × 10 Mb ST mm fiber and 2 × 100 Mb ST mm fiber
- AG module: 2 × RJ45 10/100 Mb copper and 2 × 100 Mb SC sm fiber

2.2.2 Six-port Modules

The combo six-port modules are combinations of copper and fiber media, available as four 10/100 switched RJ45 copper ports and two 100 Mb switched multi-mode fiber ST or SC ports as shown below.

- A5 module: 2 × 10 Mb ST mm fiber and 4 × RJ45 10/100 Mb copper
- A6 module: 2 × 100 Mb ST mm fiber and 4 × RJ45 10/100 Mb copper
- A7 module: 2 × 100 Mb ST sm fiber and 4 × RJ45 10/100 Mb copper
- A8 module: 2 × 100 Mb SC sm fiber (20 km) and 4 × RJ45 10/100 Mb copper
- A9 module: 2 × 100 Mb SC sm fiber (40 km) and 4 × RJ45 10/100 Mb copper

For ports numbering, ports 1, 3, 5, and 7 are copper, ports 2 and 6 are fiber, while ports 4 and 8 are not present.



754703A1.CDR

FIGURE 2–2: Two 10 Mb ST fiber and four RJ45 10/100 Mb copper

The four RJ45 ports operate just like the 8-port copper module, and the two fiber ports operate at 100 Mbps full-duplex (default). User mode control per port through the ML2400 software is also the same.

On the six-port combo modules, there are four LEDs for each RJ45 port, which indicate status the same as described in the previous section.

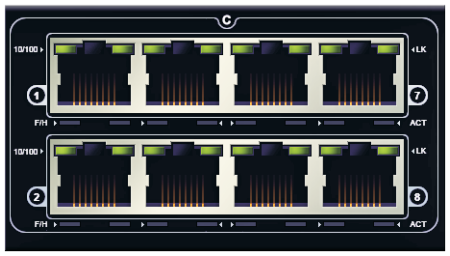
There are three LEDs per fiber port. The Link (LK) LED, when lit, indicates "ready for operation" on that port, the F/H LED indicates operation in full-duplex mode when ON (half-duplex when OFF), and the blinking ACT LED indicates receiving activity on the port. A fiber cable must be connected to the port, and the link (LK) indicator for that port must be ON (indicating there is a powered-up device at the other end of the cable) in order for a LK LED to provide valid indications of operating conditions on that port. Color-coding on the panel of the module shows which LEDs belong to which port.

The six-port modules are also available with four RJ45 10/100 copper and two 10 Mb fiber mm ST ports. For detailed information about 10Mb mm ST fiber half of the module, refer to the next section.

2.2.3 Eight-port Modules

The ML2400 8-port copper module (A4 module) provides eight 10/100 Mb switched RJ45 ports. The 10/100Mb switched ports normally (as a default setting) are independently *n*-way auto-negotiating for operation at 10 or 100 Mb speed in full or half-duplex mode; that

is, each independently selects a mode and speed to match the device at the other end of the twisted pair cable (see *Auto-Negotiation (for Fast Ethernet Copper Ports)* on page 4–2 for additional details).



754702A1.CDR

FIGURE 2–3: RJ45 10/100 Mb 8-port copper module

On this module, there are four LEDs for each port, two in the connector and two separate. The LK (Link) LED indicates "ready for operation" on that port when lit. The blinking ACT (Activity) LED indicates receiving Activity on that port when lit. The 10/100 LED indicates operation at 100 Mb speed when ON and at 10 Mb speed when OFF (when auto-negotiation is not disabled). The F/H LED is ON to indicate full-duplex operation and OFF to indicate half-duplex mode. A twisted pair cable must be connected into an RJ45 port and the Link (LK) indicator for that port must be ON (indicating there is a powered-up device at the other end of the cable) in order for a LK LED to provide valid indications of operating conditions on that port.

Using the ML2400 management software, the user may disable auto-negotiation and fix the desired operation of each RJ45 port. User may select the 10 or 100 Mb speed and full or half-duplex mode per-port as per the user requirement.

The combo eight-port modules are combinations of copper and fiber media, available in the configurations shown below.

- AA module: 4 × 100 Mb LC mm fiber (2 km) and 4 × RJ45 10/100 Mb copper
- AB module: 8 × 100 Mb LC mm fiber (2 km)
- AC module: 4 × 100 Mb LC sm fiber (15 km) and 4 × RJ45 10/100 Mb copper
- AD module: 8 × 100 Mb LC sm fiber (15 km)
- AE module: 2 × 100 Mb LC sm fiber (15 km) and 6 × RJ45 10/100 Mb copper

2.2.4 Gigabit (1000 Mbps) Modules

The 1000 Mb Gigabit fiber-port modules on the ML2400 are normally set (factory default) to operate in AUTO mode for best fiber distance and performance. The 1000 Mbps SC fiber-optic module on the Gigabit-SX and Gigabit-LX transceivers are compatible with the IEEE 802.3z Gigabit standards.

754730A1.CDR

FIGURE 2–4: Gigabit module in fourth port

2.3 Features and Benefits

2.3.1 Packet Prioritization, 802.1p QoS

Quality of Service (QoS) means providing consistent predictable data delivery to users from datagram paths that go all across a network. As a LAN device, the ML2400 can do its part to prevent any QoS degradation while it is handling Ethernet traffic through its ports and buffers.

The ML2400 switching hardware supports the IEEE 802.1p standard and fulfills its role in support of QoS, giving packet processing priority to priority tagged packets according to the 802.1p standard. In addition to hardware support for QoS, the ML2400 software supports two priority queues that can be shared across the eight levels of defined packet priorities for application-specific priority control by the user through software configuration settings.

2.3.2 Frame Buffering and Flow Control

The ML2400 is a store-and-forward switch. Each frame (or packet) is loaded into the switch's memory and inspected before forwarding can occur. This technique ensures that all forwarded frames are of a valid length and have the correct CRC, i.e., are good packets. This eliminates the propagation of bad packets, enabling all of the available bandwidth to be used for valid information.

While other switching technologies (such as “cut-through” or “express”) impose minimal frame latency, they will also permit bad frames to propagate out to the Ethernet segments connected. The “cut-through” technique permits collision fragment frames (which are a result of late collisions) to be forwarded which add to the network traffic. Since there is no way to filter frames with a bad CRC (the entire frame must be present in order for CRC to be calculated), the result of indiscriminate cut-through forwarding is greater traffic congestion, especially at peak activity. Since collisions and bad packets are more likely when traffic is heavy, the result of store-and-forward operation is that more bandwidth is available for good packets when the traffic load is greatest.

When the ML2400 detects that its free buffer queue space is low, the switch sends industry standard (full-duplex only) PAUSE packets out to the devices sending packets to cause “flow control”. This tells the sending devices to temporarily stop sending traffic, which allows a traffic catch-up to occur without dropping packets. Then, normal packet buffering and processing resumes. This flow-control sequence occurs in a small fraction of a second and is transparent to an observer.

Another feature implemented in the ML2400 is a collision-based flow-control mechanism (when operating at half-duplex only). When the switch detects that its free buffer queue space is low, it prevents more frames from entering by forcing a collision signal on all receiving half-duplex ports in order to stop incoming traffic.

2.3.3 MultiLink Switch Software

The ML2400 includes licensed software, allowing configuration of the ML2400 as a managed switch.

All software information, including new releases and upgrades, can be accessed and download from the GE Multilin website at http://www.GEmultilin.com.

2.3.4 Redundant Power Supply

With the redundant power supply, the ML2400 can receive power from either power supply 1 (A) or power supply 2 (B). The switch load is shared if both power supplies are available. The unit will not allow power to flow from a one input to another input (i.e. the two power sources are not mixed together by the switch).

When one power supply is present, the ML2400 will receive power even if the other power supply is absent, or if it is connected with reverse polarity, shorted, or grounded.

If reverse polarity connections should accidentally occur on either input, they will not damage the ML2400 or power supply (nor will it blow the fuse in the internal power supply) because of the blocking action of the diodes. This is true even if one input connection is reversed while the Switch is operating from the other source.

The ML2400 will not receive power (and will not work) when both inputs are simultaneously absent.

The status of the power supplies can be queried with the `show power` command.

show power

Power supply 1 on the switch is power input A and power supply 2 on the switch is power input B. For example,

```
ML2400# show power

  Power Input A Good.
  Power Input B Good.
```

The `show power` command is only available in switches with redundant power supplies.

2.3.5 Additional Features and Benefits

- **Managed switching for high performance Ethernet LANs**: The ML2400 provides non-blocking (all ports can run at full speed) performance with standard managed networks software included.
- **Switching services includes 802.1p QoS packet prioritization**: The ML2400 switching hardware supports QoS, giving packet processing priority to priority tagged packets according to the IEEE 802.1p standard. For port- and application-specific priorities of data, the QoS software may be configured.
- **Features fiber-built-in**: The ML2400 is designed to include fiber ports and supports mixes of multi-mode and single-mode, 10/100/1000 Mb speed, full-and half-duplex, and GBIC fiber connectors. The RJ45 10/100 ports can also be configured with the mix of port types.
- **Relay contacts for monitoring internal power and user-defined software events**: Two alarm relay contacts monitor basic operations. One is for hardware and will signal loss of power internally. The other is software controllable and will signal user-defined software events such as a security violation.
- **Modular design for port flexibility, in a 1U space-saving rack-mount package**: The 1U ML2400 chassis has four slots for port configuration. A family of 4, 6 or 8 port modules allows the user to select the desired mix of port types and speeds.

The port modules are normally factory installed and tested, but may be changed in the field.

- **Heavy-duty design for industrial Ethernet and extended temperature operation**: Fiber ports take more power than copper ports, but the ML2400 design provides for this with heavy-duty components. The ambient temperature can be up to is 85°C.
- **NEBS and ETSI tested and certified**: The ML2400 has been tested and certified for NEBS and ETSI. Test reports are available upon request.

2.4 Applications

2.4.1 Description

The MultiLink ML2400 Ethernet Switch offers high performance and modularity. It provides the flexibility of 100 Mbps fiber, copper, and Gigabit ports, with industry-standard LAN management software. The ML2400 switches are easily used in a variety of applications, including MANs (metropolitan area networks) client/server computing, secure VLAN performance upgrades to departmental networks, and LAN traffic centers requiring Gb backbone services. The performance characteristic of the ML2400 switches enable them to interconnect a series of subnets (one subnet per ML2400 port) in a LAN traffic center. The subnet connections may be via fiber or twisted pair cabling, 100 or 10 Mbps speed, and full-or half-duplex mode.

The mixed-media capability of the ML2400 is ideal for upgrading existing Ethernet LAN networks where existing cabling must be accommodated. The fiber media capability is ideal for integrating future-proof fiber cabling into the LAN structure.

2.4.2 ML2400 Switch for a VLAN Application

The MultiLink ML2400 Ethernet Switch can handle VLAN applications and provide security and performance in Ethernet network centers. A secure VLAN-enabled network is an administratively configured broadcast domain. The network administrator determines which ports and nodes belong to certain broadcast domains by setting membership profiles. The ML2400 VLAN capability can be developed in several types of virtual LANs, such as port-based or tag-based VLANs.

In an office environment where departments such as Finance, Engineering, R&D, and Marketing require a secure LAN, the ML2400 VLAN feature will prevent traffic cross-over among domains and keep sensitive data and information under control. The managed ML2400 with VLANs capability is ideal for any application where a secure VLAN is required for multiple departments.

The modularity of the ML2400 makes it an attractive choice for applications with LAN connections to an multiple site offices. Disparate offices can be easily connected with the Fiber ports supported by the ML2400 switch. A main NT-based server in a secure area, protected from earthquake or fire hazards, can be connected to the full duplex Gigabit fiber port.

Full-duplex future proof fiber media can easily connect long distance subnets and provide a stable secure network to all applications. The SNMP management capability of the ML2400 allows the creation of a database of all network subnets.

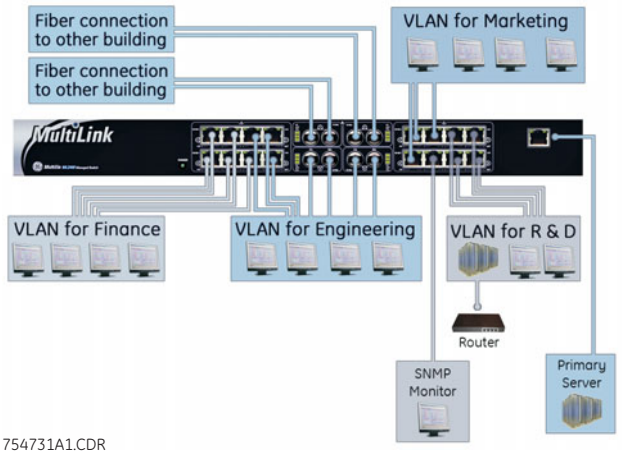


FIGURE 2–5: VLAN application

2.4.3 Network with Multiple Subnets

A managed switch is needed to provide an Ethernet backbone for a diversified network with multiple subnets. The backbone consists of high speed LAN segments supported by 100 Mbps full-duplex future-proof fiber media to provide secure long distance LAN connections. The entire network is sharing a higher bandwidth Gigabit-enabled data-mining server for the vital database located in a separate secured building. The copper ports are required for multiple subnets inside the building. The entire spread network will be manageable to provide easy, detectable, uninterrupted support through a viewable SNMP monitor.

The MultiLink ML2400 Ethernet Switch equipped with the mix of copper and fiber ports provides an economical and seamless solution to the requirements. The user-configurable ML2400 provides an extra boost to the network requirements by providing copper/fiber media along with the higher bandwidth support of 10/100 and 1000 Mb. The user can utilize the SNMP feature equipped with VLAN, RMON, SNTP and other standard managed LAN features to provide a secure and stable network.

The ML2400 managed switch with mixed-media flexibility allows the users more than one configuration alternative. The user has an advantage by fulfilling the present requirements as well as benefiting from the multiple choices of modules to support future expansion as the network evolves. The Gigabit port option boosts the bandwidth for high speed to support the peak traffic and minimize congestion.

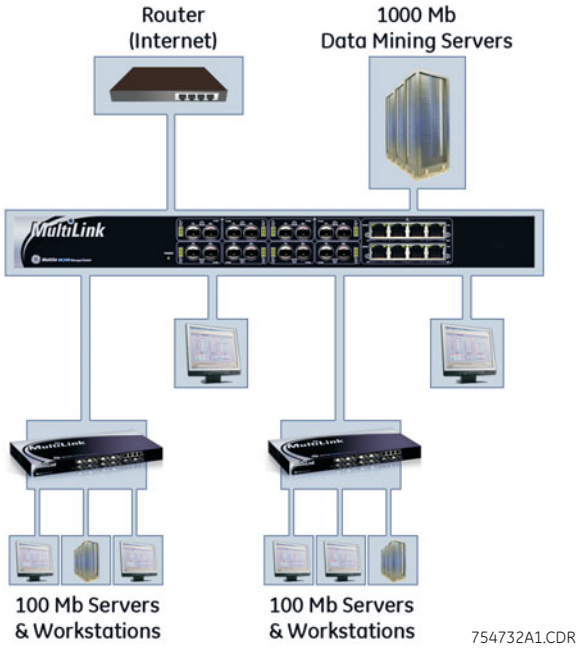


FIGURE 2–6: Network with multiple subnets example

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 3: Installation

3.1 Preparation

3.1.1 Precautions

Before installing the equipment, it is necessary to take the following precautions if the equipment is mounted in an enclosed or multiple rack assembly:

1. Ensure the environmental temperature is less than or equal to 50°C.
2. Maintain adequate air flow for proper and safe operation.
3. Placement of the equipment must not overload or unevenly load the rack system.
4. Verify the equipment's power requirements to prevent overloading of electrical circuits.
5. Verify that the equipment has a reliable and uncompromised grounding path.
6. Equipment is to be installed by service personnel in a restricted operation area.

This chapter describes installation of the MultiLink ML2400 Ethernet Switch, as well as connection of the various Ethernet media types.

3.1.2 Locating the ML2400

For mounting instructions, refer to *Mechanical Installation* on page 3–6.

The location of a ML2400 switch is dependent on the physical layout of the network. The ML2400 is typically placed in a central location where groups of network devices need to communicate. These switches are typically rack mounted in a wiring closet see Section 3.3.2 below), but because they have rubber feet they can also be installed on a shelf or table top unit. The compact size allows the ML2400 to be easily placed in an office or lab area, and it can also be either shelf of wall-mounted (see Section 3.3.1 below).

Locate an power source within six feet (2 meters) of the intended ML2400 site. The rugged metal case of the will normally protect the switch from accidental damage in a lab or workplace setting. Maintain an open view of the front to visually monitor the status LEDs.

3.2 Connecting Ethernet Media

3.2.1 Description

The ML2400 switches are specifically designed to support standard Ethernet media types within a single unit. This is accomplished by using a family of modules that are individually selected and configured.

The supported media types with the corresponding IEEE 802.3, 802.3D, 802.3u, 802.3AB and 802.3z standards and connector types are as follows:

Table 3–1: Ethernet media

IEEE standard	Media type	Distance
100Base-FX	multi-mode fiber	220 m
	single-mode fiber	5 km
10Base-T	twisted-pair	100 m
100Base-TX	100Base-FX	100 m

3.2.2 Connecting ST-type Fiber Optics (twist-lock)

The following procedure applies to installations using modules with ST-type fiber connectors. These are type A1, A2, A4, A5, A6, and A7 modules.

- **Before connecting the fiber optic cable, remove the protective dust caps from the tips of the connectors on the module.**
  Save these dust caps for future use.
- **Wipe clean the ends of the dual connectors with a soft cloth or lint-free lens tissue dampened in alcohol.**
  Ensure the connectors are clean before proceeding.

One strand of the duplex fiber optic cable is coded using color bands at regular intervals. The color-coded strand must be used on the associated ports at each end of the fiber optic segment.

- **Connect the transmit (TX) port on the module (light colored post) to the receive (RX) port of the remote device.**
  Begin with the color-coded strand of the cable for this first TX-to-RX connection.
- **Connect the receive (RX) port on the module (dark colored post) to the transmit (TX) port of the remote device.**
  Use the non-color coded fiber strand.

The LINK LED on the module will illuminate when a connection has been established at both ends (assuming power is ON). If LINK is not lit after cable connection, the cause may be improper cable polarity. Swap the fiber cables at the module connector to remedy this situation.

3.2.3 Connecting SC-type Fiber Optics (snap-in)

The following procedure applies to installations using modules with SC-type fiber connectors. These include the A3, A8, A9, and G2 modules.

When connecting fiber media to SC connectors, simply snap on the two square male connectors into the SC female jacks of the module until it clicks and secures.

3.2.4 Connecting Single-mode Fiber Optics

When using single-mode fiber cable, be sure to use single-mode fiber port connectors. Single-mode fiber cable has a smaller diameter than multi-mode fiber cable (9/125 microns for single-mode versus 50/125 or 62.5/125 microns for multi-mode, where *xx*/*xx* represent the core diameters and the core plus cladding, respectively). Single-mode fiber allows full bandwidth at longer distances and may be used to connect 10 Mb nodes up to 10 km.

The same connection procedures for multi-mode fiber apply to single-mode fiber connectors. Follow the steps listed *Connecting ST-type Fiber Optics (twist-lock)* on page 3–3.

3.2.5 Connecting RJ45 Twisted Pair

The RJ45 ports of the ML2400 can be connected to the following two media types: 100Base-TX and 10Base-T. CAT Five cables should be used when making 100Base-TX connections. When the ports are used as 10Base-T ports, CAT.3 may be used. In either case, the maximum distance for unshielded twisted pair cabling is 100 m (328 ft.).

It is recommended that high quality CAT. 5 cables (which work with 10 Mb and 100 Mb) be used whenever possible to provide flexibility in a mixed-speed network, as dual-speed ports are auto-sensing for 10 and 100 Mb/s.

The following procedure describes how to connect a 10Base-T or 100Base-TX twisted pair segment to the RJ45 port. The procedure is the same for both unshielded and shielded twisted pair cables.

- ▷ **Using standard twisted pair media, insert either end of the cable with an RJ45 plug into the RJ45 connector of the port. Even though the connector is shielded, either unshielded or shielded cables may be used.**
- ▷ **Connect the other end of the cable to the corresponding device.**
- ▷ **Use the LINK LED to ensure connectivity by noting that the LED will be illuminated when the unit is powered and connection is established.**

The ML2400 RJ45 Gigabit ports can be connected to 1000Base-T, CAT.5E (or better), 100 Ω UTP, or shielded twisted-pair (STP) balanced cable media. The CAT.5E or shielded twisted pair (STP) balanced cable is recommended when making 1000Base-TX connections. In either case, the maximum distance for unshielded twisted pair cabling is 100 m (328 ft.).

It is recommended that high quality CAT. 5E cables (which work at both 100 and 1000 Mb) be used whenever possible to provide flexibility in a mixed-speed network.

The following procedure describes how to connect a 1000Base-T twisted pair segment to the RJ45 port. The procedure is the same for both unshielded and shielded twisted pair cables.

1000Base-T connections require that all four pairs or wires be connected:

- ▷ **Insert either end of the cable with an RJ45 plug into the RJ45 connector on the module.**
  Although the connector is shielded, either unshielded or shielded cables may be used.
- ▷ **Connect the other end of the cable to the corresponding device.**
- ▷ **Use the LINK LED to ensure connectivity by noting that the LED will be illuminated when the unit is powered and connection is established.**

3.2.6 Connecting Gigabit Media using GBICs

The Gigabit ports accept industry-standard GBICs for user selection of the gigabit media type desired. A selection of fiber and copper GBICs are available.

3.3 Mechanical Installation

3.3.1 Table-top or Shelf Mounting

The MultiLink ML2400-AC Ethernet Switch can be mounted on a table-top or any suitable horizontal surface. It has four rubber feet to provide stability without scratching finished surfaces.

3.3.2 Rack Mounting

Installation of a MultiLink ML2400 Ethernet Switch in a 19-inch rack is a simple procedure. The units are 1 U (1.70") high. When properly installed, the front-mounted LED status indicators should be in plain view and easy to read. Rack-mount installation requires special 19-inch rack-mounted brackets and screws (included with the ML2400). These brackets attach to the front sides of the switch, which is then typically fastened into a standard 19" RETMA rack as shown below.

FIGURE 3–1: Rack mounting

The 23-inch brackets and the ETSI (European metric, approximately 21") brackets are also available for rack-mounting of the ML2400. These brackets are popular in the telecommunications industry where they are a standard for central office rack-mounting purposes. The 23-inch and the ETSI brackets are mainly used for larger equipment assemblies in rack-mounting frames where the rack-mount equipment is typically accessed in operation from both sides.

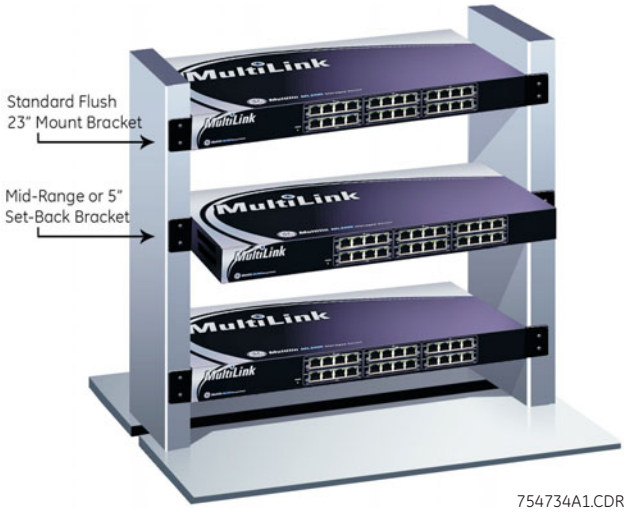


FIGURE 3–2: Mountings for ML2400 units rack-mounted in a frame

The bracket mounting holes in the sides of the ML2400 permits it to be mounted in various ways. The same holes fit all three types (19", ETSI, 23") of brackets. The mounting for the 23" is illustrated above. The brackets may be attached flush with the front, or attached in the center for a set-back mounting which may reduce cabling torque.

The optional 23" brackets and the ETSI (21") brackets each come as a pair in a package, along with the necessary screws for attaching the brackets to the sides of the ML2400. They must be ordered as line items.

3.4 Electrical Installation

3.4.1 Powering the ML2400

Units with the AC power supply option can be connected directly to 110/240 V AC with the supplied power cord.

The standard high voltage (120/125 V AC/DC) or low-voltage (48 V DC) terminal block on the ML2400 is located on the rear of the unit and is equipped with three (3) screw-down lead posts. The power terminals are identified as positive (+), negative (–), and filter ground (⏚) for DC power and as live L(+), neutral N(–), and ⏚ for AC power. These terminals are floating inside the unit so that either may be grounded by the user if desired. The chassis or safety ground is the stud located beside the terminal block.

The connection procedure is straightforward. Simply insert DC leads to the ML2400 power terminal positive (+), negative (–), and ⏚ or AC leads to the live L(+), neutral N(–), and ⏚. Please ensure the correct polarity. The ⏚ should be connected to the safety ground, except during dielectric testing. Ensure that each lead is securely tightened.

754735A3.CDR

FIGURE 3–3: Power connection and alarm contacts

NOTE

Always use a voltmeter to measure the voltage of the incoming power supply and properly determine the positive and negative leads.

NOTE

The GND should be hooked up first. The ML2400 has a floating ground, so the user may elect to ground either the positive or negative terminal.

When power is applied, the green PWR LED will illuminate.

The ML2400 is available with a redundant power supply option. If the redundant power supply is ordered, it should be wired as described above. The possible combinations of redundant power supplies are: HI-HI, HI-LO, LO-HI, and LO-LO. The AC power supply cannot be supplied with a redundant supply.

3.4.2 UL Requirements for DC-Powered Units

1. Minimum 18 AWG cable for connection to a centralized DC power source.
2. Minimum 14 AWG cable for connection to a earthing wiring.

3. Use only with listed 10 A circuit breaker provided in building installation.
4. "Complies with FDA radiation performance standards, 21 CFR sub-chapter J" or equivalent.
5. Fastening torque of the lugs on the terminal block: 9 inch-pound maximum.
6. For AC and HI powered units, use only with listed 20A circuit breaker provided in building installation. Circuit breaker shall be provided in end system or building as disconnect device.
7. Centralized DC power source cable securing; use at least four cable ties to secure the cable to the rack at least 4 inches apart, with the first one located within 6 inches of the terminal block.

3.4.3 Alarm Contacts

The alarm contacts feature provides two form-A normally closed (NC) contacts to which the user can attach two sets of status monitoring wires at the green terminal block. When this option is present, the terminal block for alarm contacts is part of the power input panel in the ML2400 case. The DC power input connection is in the same panel. A manual on-off switch for power to the unit is not available on ML2400 units with the alarm contacts option, as these two features occupy the same space in the case.

The first NC alarm contact (top position) is a "software alarm", operated by user settings in the ML2400 software. The user can disable the software alarm feature with a software configuration command if desired. When the software alarm is enabled, the form-A normally closed (NC) contact is held close during normal software operation. A user-defined software malfunction, such as an SNMP trap or a software security violation, causes the contact to open and thus trigger an alarm in the user's monitoring system

The second (bottom position) NC alarm contact is held closed when there is power on the main board inside of the ML2400. This provides a "hardware alarm" because the NC contacts will open when internal power is lost, either from an external power down condition or by the failure of the ML2400 power supply. For an ML2400 with the redundant power supply option, the hardware alarm contact will change state if any one of the power supplies fails.

Useful information about the alarm contacts:

- The four terminal block (1, 2, 3, and 4) is adjacent to the power supply.
- The top two pins (1 and 2) are software operated.
- The bottom two pins (3 and 4) are hardware operated.
- By default, the alarm contacts are NC (normally closed).
- Software operation must be enabled to get the alarm traps. Further information is provided in this manual.

The green alarm contacts are on the front rear area (next to the power source) of the ML2400 unit.

3.4.4 Dielectric Strength (hi-pot) Testing

CAUTION

The shorting link between the ⏚ and safety ground must be removed prior to the dielectric strength test to protect the transient suppression circuitry of the power supply.

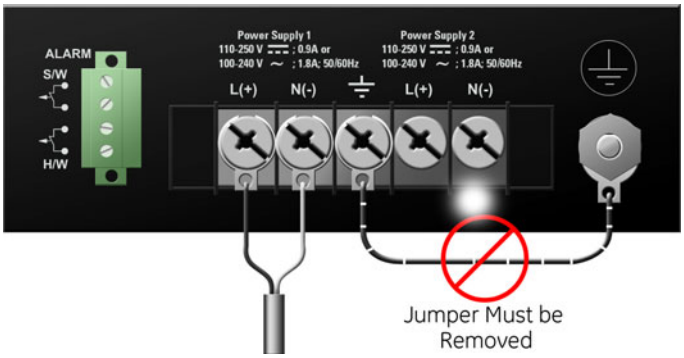


FIGURE 3–4: Dielectric strength testing

3.5 Connecting a Management Console Terminal to the ML2400

3.5.1 Description

Use a DB-9 null-modem cable or a DB-9 to USB null-modem cable to connect the ML2400 console port (the RS232 port) to the a PC.

NOTE

Console cables may be purchased as a separate items. They are not included with the unit.

754736A1.CDR

FIGURE 3–5: ML2400 console port

The pin assignment for the console port are indicated in the following table.

Table 3–2: Console port pin assignment

Pin	Signal	Description
1	CD	Carrier detect (not used)
2	RXD	Receive data (input)
3	TXD	Transmit data (output)
4	open	not used
5	GND	Signal ground
6 to 9	open	not used

This information enables a management station (PC or console terminal) to connect directly to the switch console using a straight-through serial cable.

Multilink ML2400

Ethernet Communications Switch

Chapter 4: Operation

4.1 Functionality

4.1.1 Switching Functionality

The MultiLink ML2400 provides switched connectivity at Ethernet wire-speed. The ML2400 supports10/100 Mbps for copper media and 10 or 100 Mb separate traffic domains for fiber ports to maximize bandwidth utilization and network performance. All ports can communicate to other ports in a ML2400, but local traffic on a port will not consume any of the bandwidth on any other port.

The ML2400 is a plug-and-play device. There is no software configuration necessary for basic operation, installation, or maintenance. Optional half/full-duplex mode and 10 or 100 Mbps selection for the switched ports must be configured through software as per the requirement. The internal functions of both are described below.

4.1.2 Filtering and Forwarding

Each time a packet arrives on one of the switched ports, the decision is taken to either filter or to forward the packet. Packets whose source and destination addresses are on the same port segment will be filtered, constraining them to that one port and relieving the rest of the network from having to process them. A packet whose destination address is on another port segment will be forwarded to the appropriate port, and will not be sent to the other ports where it is not needed. Traffic needed for maintaining the un-interrupted operation of the network (such as occasional multi-cast packets) are forwarded to all ports.

The ML2400 operates in the store-and-forward switching mode, which eliminates bad packets and enables peak performance when there is heavy traffic on the network.

4.1.3 Address Learning

All ML2400 units have address table capacities of 4K node addresses suitable for use in larger networks. They are self-learning, so as nodes are added, removed or moved from one segment to another, the ML2400 automatically keeps up with node locations.

An address-aging algorithm causes least-used addresses to fall out in favor of frequently-used addresses. To reset the address buffer, cycle power down-and-up.

4.1.4 Status LEDs

The following status LEDs are included:

- PWR: Power LED, ON when external power is applied to the unit.
- LK: Steady ON, link status for 10 Mbps and 100 Mbps operation.
- ACT: ON with port activity for 10 Mbps and 100 Mbps operation.
- F/H: Full/half-duplex LED, ON when the port is running full-duplex, OFF for half-duplex.
- 100/10: Speed LED, ON when the speed is 100 Mbps, OFF when the speed is 10 Mbps.

4.1.5 Up-link Manual Switches (for RJ45 port only)

The module has a manual up-link switch, located on the inside of the board next to the 10/100Mb (RJ45) port # 1 which it controls. It enables the port's cable to be cascaded (X) to a 10/100Mb repeater or switching hub in the network. The Up-link Switch position is configured as (=) straight position by default from the factory settings on all the RJ45 ports, either used for all copper module or combo module.

4.1.6 Auto-Negotiation (for Fast Ethernet Copper Ports)

The managed ML2400 Fast Ethernet copper ports can be set for either fixed 100 Mb speed or for 10/100 full/half-duplex *n*-way auto-negotiation per the IEEE802.3u standard. The selection is made via the ML2400 software. The factory default setting is for auto-negotiation. At 10 or 100 Mb fixed speed, the user may select half or full-duplex mode via software for each RJ45 port.

A common application for the ML2400 copper ports is for connection via a fiber media converter to another switch in the network backbone (or some other remote 100 Mb device). In this case, it is desirable to operate the fiber link at 100 Mb, and at either half or full-duplex mode depending on the capabilities of the remote device. Standard commercially available Fast Ethernet media converters mostly do not support auto-negotiation properly, and require that the switched port to which they are connected be at 100 Mb fixed speed. Attachment to 10/100 auto-negotiation ports typically will not work properly. The ML2400 RJ45 ports handle this situation by configuring the ports as per the software port settings and can check the port status of each port after the change.

When the ML2400 copper ports are set for auto-negotiation and are connected to an auto-negotiating device, there are four speed and F/H modes available, depending on what the other device supports. These are:

- 100Mb full-duplex

- 100Mb half-duplex
- 10 Mb full-duplex
- 10 Mb half-duplex

The auto-negotiation logic will attempt to operate in descending order and will normally arrive at the highest order mode that both devices can support at that time. (Since auto-negotiation is potentially an externally controlled process, the original "highest order mode" result can change at any time depending on network changes that may occur). If the device at the other end is not an auto-negotiating device, the ML2400 RJ45 ports will try to detect its idle signal to determine 10 or 100 speed, and will default to half-duplex at that speed per the IEEE standard.

Auto-negotiation per-port for 802.3u-compliant switches occurs when:

- Devices at both ends of the cable are capable of operation at 10 Mb or 100 Mb and/or in full/half-duplex mode, and can send/receive auto-negotiation pulses, **and**
- The second of the two connected devices is powered up (i.e., when LINK is established for a port) **or** the LINK is re-established on a port after being lost temporarily.

Some NIC cards only auto-negotiate when the computer system that they are in is powered up. These are exceptions to the "negotiate at LINK enabled" rule above, but may be occasionally encountered.

When operating in 100 Mb half-duplex mode, cable distances and hop-counts may be limited within that collision domain. The Path Delay Value (PDV) bit-times must account for all devices and cable lengths within that domain. For MultiLink fast Ethernet switched ports operating at 10 0Mb half-duplex, the bit time delay is 50BT.

4.1.7 Flow Control (IEEE 802.3x)

The ML2400 incorporates a flow-control mechanism for full-duplex mode. Flow-control reduces the risk of data loss if a long burst of activity causes the switch to save frames until its buffer memory is full. This is most likely to occur when data is moving from a 100 Mb port to a 10 Mb port and the 10 Mb port is unable to keep up. It can also occur when multiple 100 Mb ports are attempting to transmit to one 100 Mb port, and in other protracted heavy traffic situations.

The ML2400 implements the 802.3x flow control (non-blocking) on full-duplex ports, which provides for a "PAUSE" packet to be transmitted to the sender when the packet buffer is nearly filled and there is danger of lost packets. The transmitting device is commanded to stop transmitting into the ML2400 port for sufficient time to let the Switch reduce the buffer space used. When the available free-buffer queue increases, the Switch will send a "RESUME" packet to tell the transmitter to start sending the packets. Of course, the transmitting device must also support the 802.3x flow control standard in order to communicate properly during normal operation.

In half-duplex mode, the ML2400 implements a back-pressure algorithm on 10/100 Mb ports for flow control. That is, the switch prevents frames from entering the device by forcing a collision indication on the half-duplex ports that are receiving. This temporary "collision" delay allows the available buffer space to improve as the switch catches up with the traffic flow.

4.1.8 Power Budget Calculations with Fiber Media

Receiver sensitivity and transmitter power are the parameters necessary to compute the power budget. To calculate the power budget of different fiber media installations using MultiLink products, the following equations should be used:

$$OPB = P_{t(min)} - P_{R(min)} \quad \textbf{(EQ 4.1)}$$

where: OPB = optical power budget
P_T = transmitter output power
P_R = Receiver Sensitivity

The worst case OPB is as follows:

$$OPB_{worst} = OPB - 1dB\ (LED\ aging) - 1dB\ (insertion\ loss) \quad \textbf{(EQ 4.2)}$$

The worst-case distance is calculated as follows:

$$distance_{worst} = \frac{worst\text{-}case\ OPB\ (in\ dB)}{cable\ loss\ (in\ dB/km)} \quad \textbf{(EQ 4.3)}$$

The cable loss in dB/km is defined in the following table:

Table 4–1: Cable losses

Cable size	Mode	Cable loss
62.5 / 125 µm	multi-mode	2.8 dB/km
50 / 125 µm	multi-mode	2.8 dB/km
100 / 140 µm	multi-mode	3.3 dB/km
9 / 125 µm	single-mode	0.5 dB/km 0.4 dB/km (LXSC25) 0.25 dB/km (LXSC40) 0.2 dB/km (LXSC70)

The following data has been collected to provide guidance to network designers and installers.

Table 4–2: Power budget values for various modules

Module	Speed	Mode	fdx (hdx)	λ	Size	P_T	P_R	OPB_{worst}	d_{worst}	OPB_{typ}	$d_{typical}$
A1, A5	10 Mb FL	multi	2 (2) km	850 nm	62.5/125 µm 100/140 µm 50/125 µm	-15.0 dB -9.5 dB -19.5 dB	-31 dB -31 dB -31 dB	14 dB 19.5 dB 19.5 dB	5.0 km 5.9 km 3.4 km	17 dB 23.5 dB 13.2 dB	6.0 km 7.0 km 4.8 km
A2, A3, A6	100 Mb FX	multi	2 (0.4) km	1300 nm	62.5/125 µm 50/125 µm	-20 dB- 23.5 dB	-31 dB -31 dB	9.0 dB 5.5 dB	3.0 km 2.0 km	14 dB 12 dB	5.0 km 4.0 km
A7, A8	100 Mb FX	single	18+ (0.4) km	1300 nm	9/125 µm	-15 dB	-31 dB	14 dB	28 km	17.5 dB	35 km
AA, AB	100 Mb FX	multi	2 (0.4) km	1310 nm	62.5/125 µm	-19 dB	-31 dB	12 dB	4.0 km	16 dB	5.7 km
AC, AD, AE	100 Mb FX	single	15+ km	1310 nm	9/125 µm	-15 dB	-28 dB	11 dB	22 km	--	--
AF	10 Mb FL	multi	2 (2) km	850 nm	62.5/125 µm 100/140 µm 50/125 µm	-15.0 dB -9.5 dB -19.5 dB	-31 dB -31 dB -31 dB	14 dB 19.5 dB 9.5 dB	5.0 km 5.9 km 3.4 km	17 dB 23.5 dB 13.5 dB	6.0 km 7.0 km 4.8 km
AG	100 Mb FX	single	18+ (0.4) km	1310 nm	9/125 µm	-20 dB	-31 dB	9.0 dB	18 km	12.5 dB	25 km
G7	1000 Mb	multi	0.55 km	1310 nm	62.5/125 µm 50/125 µm	-9.5 dB	-17 dB	5.5 dB	2 km	12.5 dB	4 km
G8	1000 Mb FX	single	10 km	1310 nm	9/125 µm	-9.5 dB	-20 dB	8.5 dB	17 km	10.5 dB	21 km
G9, GM	1000 Mb FX	single	25 km	1310 nm	9/125 µm	-4.0 dB	-21 dB	15 dB	38 km	17.5 dB	43 km
GA	1000 Mb FX	single	40 km	1310 nm	9/125 µm	-4.0 dB	-21 dB	15 dB	60 km	17.5 dB	70 km
GB	1000 Mb FX	single	70 km	1310 nm	9/125 µm	-3.0 dB	-23 dB	18 dB	90 km	20.5 dB	102 km

The use of either multi-mode or single-mode fiber to operate at 100 Mbps speed over long distances (i.e., in excess of 400 m) can be achieved only if the following are applied:

1. The 100 Mb fiber segment must operate in full-duplex (FDX) mode (i.e. the full-duplex (factory default).
2. The worst-case OPB of the fiber link must be greater than the fiber cable's passive attenuation, where attenuation is the sum of cable loss, LED aging loss, insertion loss, and safety factor.

4.2 Troubleshooting

4.2.1 Overview

All MultiLink Ethernet products are designed to provide reliability and consistently high performance in all network environments. The installation of a ML2400 is a straightforward procedure (see chapter 2 for details)

Should problems develop during installation or operation, this section is intended to help locate, identify and correct these types of problems. Please follow the suggestions listed below prior to contacting your supplier. However, if you are unsure of the procedures described in this section or if the ML2400 is not performing as expected, do not attempt to repair the unit; instead contact your supplier for assistance or contact GE Multilin.

4.2.2 Before Calling for Assistance

1. If difficulty is encountered when installing or operating the unit, refer to chapter 2. Also ensure that the various components of the network are interoperable.
2. Check the cables and connectors to ensure that they have been properly connected and the cables/wires have not been crimped or in some way impaired during installation (about 90% of network downtime can be attributed to wiring and connector problems.)
3. If the problem is isolated to a network device other than the ML2400, it is recommended that the problem device be replaced with a known good device. Verify whether or not the problem is corrected. If not, go to the next step. If the problem is corrected, the ML2400 and its associated cables are functioning properly.
4. If the problem continues after completing the previous step, contact GE Multilin.

4.2.3 When Calling for Assistance

Please be prepared to provide the following information:

1. A complete description of the problem, including the following: the nature and duration of the problem, situations when the problem occurs, the components involved in the problem, and any particular application that appears to create the problem.
2. An accurate list of GE product model(s) involved, with serial number(s). Include the date(s) that you purchased the products from your supplier.
3. It is useful to include other network equipment models and related hardware, including personal computers, workstations, terminals and printers; plus, the various network media types being used.
4. A record of changes that have been made to your network configuration prior to the occurrence of the problem. Any changes to system administration procedures should all be noted in this record.

Multilink ML2400

Ethernet Communications Switch

Chapter 5: IP Addressing

5.1 IP Address and System Information

5.1.1 Overview

It is assumed that the user has familiarity with IP addresses, classes of IP addresses and related netmask schemas (for example, class A, B, and C addressing).

Without an IP address, the switch operates as a standalone Layer 2 switch. Without an IP address, you cannot:

- Use the web interface to manage the switch
- Use telnet to access the CLI
- Use any SNMP Network Management software to manage the switch
- Use NTP protocol or an NTP server to synchronize the time on the switch
- Use TFTP or FTP to download the configurations or upload software updates
- Run ping tests to test connectivity

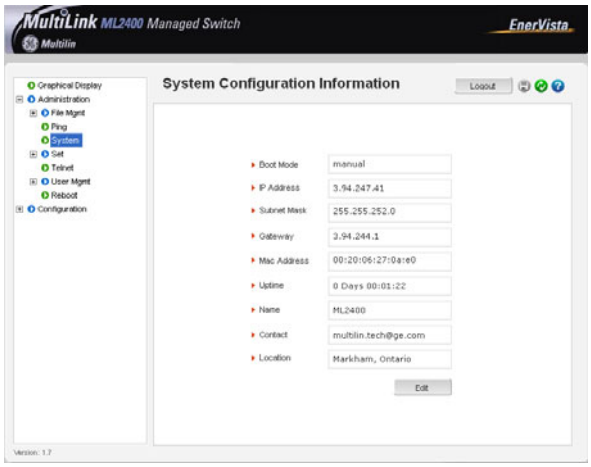
To set the IP address, please refer to *Setting the IP Parameters* on page 1–12. Once the IP address is set, the CLI can be accessed via telnet as well as the console interface. From now on, all commands discussed are accessible from the command line interface, irrespective of access methods (i.e. serial port or in band using telnet).

To verify the IP address settings using the command line interface, the `show ipconfig` command can be used as follows:

```
ML2400> show ipconfig

  IP Address:      3.94.247.41
  Subnet Mask:     255.255.252.0
  Default Gateway: 3.94.244.1

ML2400>
```

To verify the IP address using the EnerVista Secure Web Management software,

- ▷ Select the **Administration > System** menu item to view.
- ▷ Edit the IP address information.



Besides manually assigning IP addresses, there are other means to assign an IP address automatically. The two most common procedures are using DHCP and bootp.

5.2 Importance of an IP Address

5.2.1 DHCP and bootp

DHCP is commonly used for setting up addresses for computers, users and other user devices on the network. bootp is the older cousin of DHCP and is used for setting up IP addresses of networking devices such as switches, routers, VoIP phones and more. Both of them can work independent of each other. Both of them are widely used in the industry. It's best to check with your network administrator as to what protocol to use and what the related parameters are. DHCP and bootp require respective services on the network. DHCP and bootp can automatically assign an IP address. It is assumed that the reader knows how to setup the necessary bootp parameters (usually specified on Linux/UNIX systems in the `/etc/boopttab` directory).

5.2.2 bootp Database

Bootp keeps a record of systems supported in a database - a simple text file. On most systems, the **bootp** service is not started as a default and has to be enabled. A sample entry by which the **bootp** software will look up the database and update the IP address and subnet mask of the switch would be as follows:

```
ML2400:\
ht=ether:\
ha=002006250065:\
ip=3.94.247.41:\
sm=255.255.252.0:\
gw=3.94.244.1:\
hn:\
vm=rfc1048
```

where:

- `ML2400` is a user-defined symbolic name for the switch.
- `ht` is the hardware type. For the MultiLink family of switches, set this to `ether` (for Ethernet). **This tag must precede the `ha` tag**.
- `ha` is the hardware address. Use the switch's 12-digit MAC address.
- `ip` is the IP address to be assigned to the switch.
- `sm` is the subnet mask of the subnet in which the switch is installed.

Each switch should have a unique name and MAC address specified in the **bootptab** table entry

5.2.3 Configuring DHCP/bootp/Manual/AUTO

By default, the switch is configured for auto IP configuration. DHCP/bootp/manual can be enabled with the command line interface by using the `set bootmode` command with the following syntax:

set bootmode=*<dhcp|bootp|manual|auto> bootimg=<enable|disable> bootcfg=<enable|disable>*

The **bootimg** argument is only valid with the **bootp** type. This option allows the switch to load the image file from the bootp server. This is useful when a new switch is placed on a network and the IT policies are set to load a specific image which is supported and tested by IT personnel.

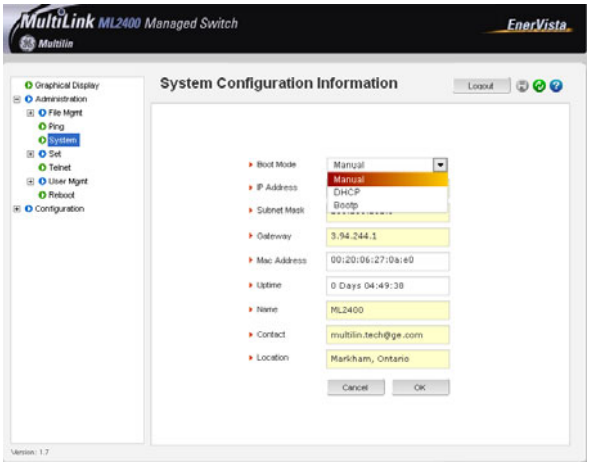
Likewise, the **bootcfg** argument is valid only with the bootp type. This option allows the switch to load the configuration file from the bootp server. This is useful when a new switch is put on a network and the specific configurations are loaded from a centralized bootp server

The following example changes the boot mode of the switch:

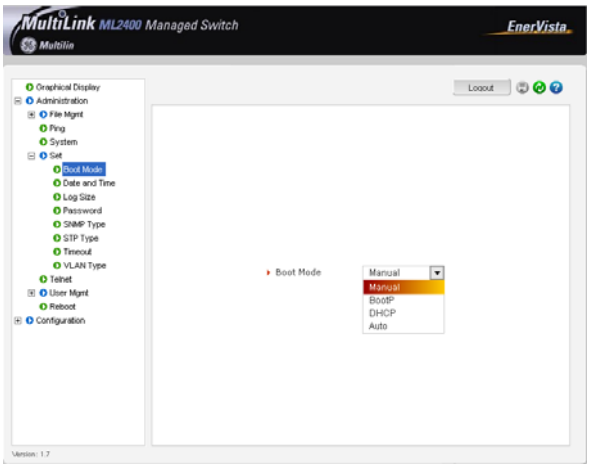
```
ML2400# set bootmode type=bootp bootimg=enable bootcfg=disable
Network application image download is enabled.
Network application config download is disabled.
Save Configuration and Restart System
ML2400#
```

Alternatively, the DHCP/bootp/manual can be enabled through the EnerVista Secure Web Management software as shown below.

- ▷ Select the **Administration > System** menu item.
- ▷ Click **Edit**.



- ▷ Alternatively, select items in the **Administration > Set** menu to individually modify the boot mode, date and time, log size, etc.



▷ **After the changes are completed for each section, click OK to register the changes.**

Note that if the IP address is changed, the `http` session has to be restarted with the new IP address.

5.2.4 Using Telnet

The telnet client is enabled on the ML2400. The ML2400 supports five simultaneous sessions on a switch: four telnet sessions and one console session. This allows many users to view, discuss, or edit changes to the ML2400. This is also useful when two remote users want to view the switch settings. The telnet client can be disabled through the command line interface by using the `telnet disable` command with the following syntax:

telnet *<enable|disable>*

Telnet can also be disabled for specific users with the `useraccess` command. Refer to *User Management* on page 1–14 for details.

Multiple telnet sessions started from the CLI interface or the command line are serviced by the ML2400 in a round-robin fashion (that is, one session after another). If one telnet session started from an ML2400 is downloading a file, the other windows will not be serviced until the file transfer is completed.

The following example changes the telnet access. In this case, the enable command was repeated without any effect to the switch.

```
ML2400# configure access
ML2400(access)## telnet enable
  Access to Telnet already enabled
ML2400(access)## exit
ML2400#
```

The `show console` command can show the status of the telnet client as well as other console parameters. The following example reviews the console parameters with the `show console` command. Note that telnet is enabled.

```
ML2400# show console
Console/Serial Link
```

```
Inbound Telnet Enabled: Yes
Outbound Telnet Enabled: Yes
Web Console Enabled: Yes
SNMP Enabled: Yes
Terminal Type: VT100
Screen Refresh Interval (sec): 3
Baud Rate: 38400
Flow Control: None
Session Inactivity Time (min): 10
```

ML2400#

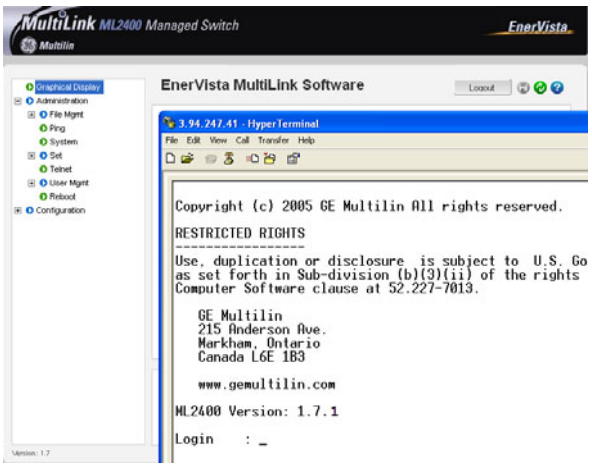
Users can telnet to a remote host from the MultiLink family of switches using the following syntax.

telnet <ipaddress> [port=<port number>]

The default port for telnet is 23.

To start a telnet session through the EnerVista Secure Web Management software,

▷ Select the **Administration > Telnet** menu item.



The default port for telnet is 23.

The ML2400 will time out an idle telnet session. It may be useful to see who is currently connected to the switch. It may also be useful for a person to remotely terminate a telnet session. To facilitate this, the ML2400 supports the following two commands:

show session
kill session *id=<session>*

For example:

```
ML2400# user
ML2400(user)## useraccess user=peter service=telnet enable
Telnet Access Enabled.
ML2400(user)## exit
ML2400# show session
```

```
Current Sessions:

SL# Sessn Id  Connection    User Name  User Mode
1   1         163.10.10.14  manager    Manager
2   2         163.11.11.1   peter      Manager
3   3         163.12.12.16  operator   Operator

ML2400# kill session id=3

Session Terminated

ML2400#
```

In the above example, the user with username "peter" is given telnet access. Then multiple users telnet into the switch. This is shown using the `show session` command. The user operator session is then terminated using the `kill session` command.

A maximum of four simultaneous telnet sessions are allowed at any time on the switch. The commands in these telnet windows are executed in a round robin fashion; that is, if one window takes a long time to finish a command, the other windows may encounter a delay before the command is completed. For example, if one window is executing a file download, the other windows will not be able to execute the command before the file transfer is completed. As well, if a outbound telnet session is started from the switch (through a telnet window) then other windows will not be able to execute a command until the telnet session is completed.

5.3 Setting Parameters

5.3.1 Setting Serial Port Parameters

To be compliant with IT or other policies the console parameters can be changed from the CLI interface. This is best done by setting the IP address and then telnet over to the switch. Once connected using telnet, the serial parameters can be changed. If you are using the serial port, remember to set the VT-100 emulation software properties to match the new settings.

The serial port parameters are modified using the `set serial` command with the following syntax:

```
set serial [baud=<rate>] [data=<5|6|7|8>] [parity=<none|odd|even>]
[stop=<1|1.5|2>] [flowctrl=<none|xonxoff>]
```

Where `<rate>` = standard supported baud rates.

Changing these parameters through the serial port will cause loss of connectivity. The terminal software parameters (e.g. HyperTerminal) will also have to be changed to match the new settings.

To see the current settings of the serial port, use the `show serial` command to query the serial port settings as illustrated below.

```
ML2400# show serial

  Baud Rate: 38400
  Data: 8
  Parity: No Parity
  Stop: 1
  Flow Control: None
```

5.3.2 System Parameters

The system parameters can be queried and changed. To query the system parameters, two commands are frequently used: `show sysconfig` and `show setup`. Usage for both commands is illustrated below.

The following example lists system parameters using the `show setup` command. Most parameters here cannot be changed.

```
ML2400# show setup

  Version: ML2400 build 1.6.1 Apr 29 2005 11:10:13
  MAC Address: 00:20:06:27:0a:e0
  IP Address: 3.94.247.41
  Subnet Mask: 255.255.252.0
  Gateway Address: 3.94.244.1
  CLI Mode: Manager
  System Name: ML2400
  System Description: 25 Port Modular
    Ethernet Switch
  System Contact: multilin.tech@ge.com
  System Location: Markham, Ontario
  System ObjectId: 1.3.6.1.4.1.13248.12.7

ML2400#
```

The following example lists system parameters using the `show sysconfig` command. Most parameters here can be changed.

ML2400# `show sysconfig`

```
System Name: ML2400
System Contact: multilin.tech@ge.com
System Location: Markham, Ontario
Boot Mode: manual
Inactivity Timeout(min): 120
Address Age Interval(min): 300
Inbound Telnet Enabled: Yes
Web Agent Enabled: Yes
Time Zone: GMT-05hours:00minutes
Day Light Time Rule: Canada
System UpTime: 7 Days 12 Hours 30 Mins 46
  Secs
```

ML2400#

System variables can be changed. Below is a list of system variables which GE recommends changing.

- `System Name`: Using a unique name helps you to identify individual devices in a network.
- `System Contact` and `System Information`: This is helpful for identifying the administrator responsible for the switch and for identifying the locations of individual switches.

To set these variables, change the mode to be SNMP configuration mode from the manager mode using the following syntax

snmp

setvar *[sysname|syscontact|syslocation] =<string>*

The following command sequence sets the system name, system location and system contact information.

ML2400# `snmp`

ML2400(snmp)## `setvar ?`

```
setvar: Configures system name, contact or
  location
Usage: setvar
 [sysname|syscontact|syslocation]=<string>
```

ML2400(snmp)## `setvar syslocation=Fremont`

```
System variable(s) set successfully
```

ML2400(snmp)## `exit`

ML2400#

5.3.3 Date and Time

It may be necessary to set the day, time or the time zone manually. This can be done by using the `set` command with the necessary date and time options with the following syntax:

set *timezone GMT=[+ or -] hour=<0-14>*

min=<0-59>

set *date year=<2001-2035> month=<1-12> day=<1-31>*
[format=<mmddyyyy|ddmmyyyy|yyyymmdd>]

set *time hour=<0-23> min=<0-59> sec=<0-59> [zone=GMT[+/-]hh:mm]*

To set the time to be 08:10 am in the -5 hours from GMT (Eastern Standard Time) and to set the date as 11 May 2005, the following sequence of commands are used.

```
ML2400# set time hour=8 min=10 sec=0 zone=GMT-5:00
  Success in setting device time
ML2400# show time
  Time: 8:10:04
ML2400# show timezone
  Timezone: GMT-05hours:00minutes
ML2400# set date year=2005 month=5 day=11
  Success in setting device date
ML2400# show date
  System Date: Wednesday 15-11-2005 (in mm
  -dd-yyyy format)
ML2400#
```

The syntax for other date and time commands are:

set timeformat *format=<12|24>*

set daylight *country=<country name>*

The following command sequence sets the daylight location:

```
ML2400# set daylight country=Canada
  Success in setting daylight savings to the
  given location/country Canada
ML2400# show daylight
  Daylight savings location name: Canada
ML2400#
```

The date and time can only be set through the command line interface software.

5.3.4 Network Time

Many networks synchronize the time using a network time server. The network time server provides time to the different machines using the Simple Network Time Protocol (SNTP). To specify the SNTP server, one has to

1. Set the IP parameters on the switch
2. Define the SNTP parameters

To set the SNTP parameter with the command line software, enter the SNTP configuration mode from the manager. The `setsntp`, `sync`, and `sntp` commands can then be used to setup the time synchronization automatically from the SNTP server. Note it is not sufficient to setup the SNTP variables. Make sure to setup the synchronization frequency as well as enable SNTP. The syntax for the above commands is shown below.

setsntp *server = <ipaddress> timeout = <1-10> retry = <1-3>*

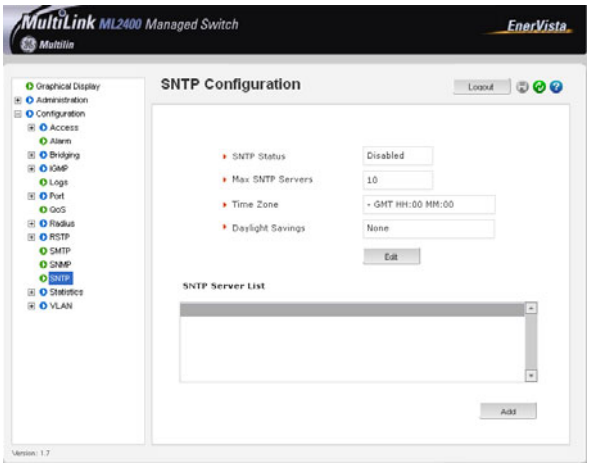
sync *[hour=<0-24>] [min=<0-59>] (default = 24 hours)*

sntp *[enable|disable]*

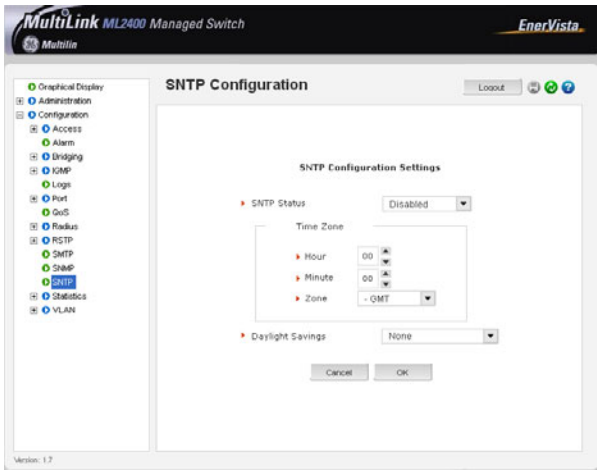
To set the SNTP server to be 3.94.210.5 (with a time out of 3 seconds and a number of retries set to 3 times); allowing the synchronization to be ever 5 hours, the following sequence of commands are used

```
ML2400# sntp
ML2400(sntp)## setsntp server=3.94.210.5 timeout=3 retry=3
  SNTP server is added to SNTP server
  database
ML2400(sntp)## sync hour=5
ML2400(sntp)## sntp enable
  SNTP is already enabled.
ML2400(sntp)## exit
ML2400(sntp)#
```

SNTP parameters can be configured through the EnerVista Secure Web Management software with the **Configuration > SNTP** menu item. The SNTP menu allows the time zone (hours from GMT) to be defined along with other appropriate parameters on setting the time and synchronizing clocks on network devices.



The **edit** button allows editing of the SNTP parameters as shown below. Adding or deleting SNTP servers is accomplished by using the add and delete buttons. Clicking the edit button allows the specific SNTP parameter settings to be modified.

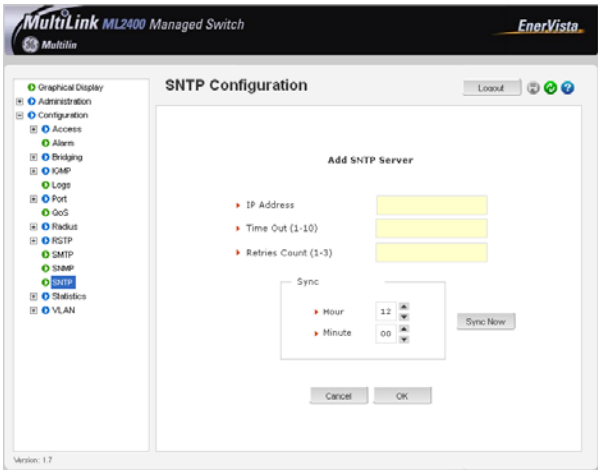


After the proper SNTP values are entered, click **OK** to register the changes, or click **Cancel** to back out from the changes made.

To add an SNTP server, click the **add** button on the **Configuration > SNTP** menu. The menu prompts you to add IP address of an SNTP server, the time out in seconds and the number of retries, before the time synchronization effort is aborted. The **Sync Now** button allows synchronization as soon as the server information is added.

NOTE

If your site has internet access, there are several SNTP servers available online. A quick search will yield information about these servers. You can use the IP address of these servers; however, please ensure the server can be reached by using the `ping` command. The `ping` command can also be launched from the EnerVista software.



The **Time Out** value is in seconds. Note the time server can be a NTP server available on the Internet. Ensure the IP parameters are configured for the switch and the device can be pinged by the switch. Once the server is added, it is listed with the other SNTP servers.

5.4 System Configuration

5.4.1 Saving and Loading – Command Line

Place the Switch offline while transferring Setting Files to the Switch.
When transferring Settings Files from one Switch to another, the IP address of the originating Switch will also be transferred. The user must therefore reset the IP address on the receiving Switch before connecting to the network.

Configuration changes are automatically registered but not saved; that is, the effect of the change is immediate. However, if power fails, the changes are not restored unless they saved using the `save` command. It is also a good practice to save the configuration on another network server using the tftp or ftp protocols. Once the configuration is saved, it can be loaded to restore the settings. At this time, the saved configuration parameters are not in a human readable format. The commands for saving and loading configurations on the network are:

saveconf *mode=<serial|tftp|ftp>*
<ipaddress> file=<name>

loadconf *mode=<serial|tftp|ftp>*
<ipaddress> file=<name>

Ensure the machine specified by the IP address has the necessary services running. For serial connections, x-modem or other alternative methods can be used. In most situations, the filename must be a unique, since overwriting files is not permitted by most ftp and tftp servers (or services). Only alphanumeric characters are allowed in the filename.

The following example illustrated how to save the configuration on a tftp server

```
ML2400# saveconf mode=tftp 3.94.240.9 file=ml2400set

Do you wish to upload the configuration?
['Y' or 'N'] Y
```

The `saveconf` and `loadconf` commands are often used to update software. Before the software is updated, it is advised to save the configurations. The re-loading of the configuration is not usually necessary; however, in certain situations it maybe needed and it is advised to save configurations before a software update. The `loadconf` command requires a reboot for the new configuration to be active. Without a reboot the older configuration is used by the MultiLink family of switches.

The `saveconf` and `loadconf` commands are often used to update software to the ML2400. These commands will be deprecated in the upcoming release and replaced with the `ftp`, `tftp`, or `xmodem` commands. It is advised to begin using these commands instead of `saveconf` and `loadconf`.

5.4.2 Config file

MNS can now use the ftp or tftp (or xmodem if using the CLI) to upload and download information to a server running the proper services. One useful capability provided in MNS is export of the CLI commands used to configure the switch. To do this, use Config Upload/ Download.

Using **Config Download**, examination of the contents of the saved file would appear as shown below:

```
<ML2400 -conf-1.0>
######################################################################
# Copyright (c) 2001-2005 GE Multilin, Inc All rights reserved.
# RESTRICTED RIGHTS
# -------------------------------
# Use, duplication or disclosure is subject to U.S. Government
# restrictions as set forth in Sub-division (b)(3)(ii) of the
# rights in Technical Data and Computer Software clause at
# 52.227-7013.
#
# This file is provided as a sample template to create a backup
# of GE MultiLink switches. As such, this script
# provides insights into the configuration of GE MultiLink
# switches settings. GE Multilin, Inc. recommends that modifications of this
# file and the commands should be verified by the User in a
# test environment prior to use in a "live" production network.
# All modifications are made at the User's own risk and are
# subject to the limitations of the GE MultiLink software End User
# License Agreement (EULA). Incorrect usage may result in
# network shutdown. GE Multilin, Inc. is not liable for incidental or
# consequential damages due to improper use.
######################################################################
***This is a Machine Generated File.
***Only the SYSTEM config block is editable.
***Editing any other block will result in error while loading.
############################################################
# Hardware Configuration - This area shows the type of          #
#                 hardware and modules installed.                                  #
############################################################
[HARDWARE]
type=ML2400
slotB=8 Port TP Module
############################################################
# System Manager - This area configures System related          #
#  information.                                                                    #
############################################################
```

```
[SYSTEM]
***Edit below this line only***

system_name=ML2400
system_contact=support@gemultilin.com
system_location= Markham, Ontario
boot_mode=manual
system_ip=192.168.5.5
system_subnet=0.0.0.0
system_gateway=0.0.0.0
idle_timeout=10
telnet_access=enable
snmp_access=enable

web_access=enable

***Edit above this line only***
#############################################################
# User Accounts - This area configures user accounts for #
#              accessing this system.              #
#############################################################
...
```

FIGURE 5–1: Contents of a config file

1. A config file allows only certain portions of the file to be edited by a user. Changing any other part of the file will result in the system not allowing the file to be loaded, as the CRC computed and stored in the file would not be matched. Should you want to edit, edit the System portion of the file only. GE Multilin, Inc. recommends editing the "script" file (see below)
2. File names cannot have special characters such as *#!@$^&* space and control characters.

5.4.3 Displaying configuration

Using SWM, the need to display specific CLI commands for configuring capabilities is not needed. The menus are modular and are alphabetically sorted to display each necessary component in a logical manner. This section is repeated from the CLI manual, should the need arise to view the necessary commands. The best way to view these commands is to telnet to the switch using the Telnet menu from the Administration menu.

To display the configuration or to view specific modules configured, the '**show config**' command is used as described below.

Syntax **show config [module=<module-name>]**

Where module-name can be:

Name	Areas affected
system	IP Configuration, Boot mode, Users settings (e.g. login names, passwords)
event	Event Log and Alarm settings
port	Port settings, Broadcast Protection and QoS settings
bridge	Age time setting
stp	STP, RSTP and LLL settings
ps	Port Security settings
mirror	Port Mirror settings
sntp	SNTP settings
llan	VLAN settings
gvrp	GVRP settings
snmp	SNMP settings
web	Web and SSL/TLS settings
tacacs	TACACS+ settings
auth	802.1x Settings
igmp	IGMP Settings
smtp	SMTP settings

If the module name is not specified the whole configuration is displayed.

```
ML2400# show config
[HARDWARE]
type= ML2400
slotB=8 Port TP Module
############################################################
```

```
# System Manager - This area configures System related          #
#              information.                                                  #
################################################################
[SYSTEM]
***Edit below this line only****
system_name=Main
system_contact=someone@joe.com
system_location= Markham, Ontario
boot_mode=manual
system_ip=192.168.1.15
system_subnet=0.0.0.0
system_gateway=192.168.1.11
idle_timeout=10
telnet_access=enable
snmp_access=enable
web_access=enable

--more—
...
```

FIGURE 5–2: 'show config' command output

```
ML2400# show config module=snmp
[HARDWARE]
type= ML2400
slotB=8 Port TP Module
#############################################################
# Network Management - This area configures the SNMPv3      #
#                agent.                                     #
#############################################################
[SNMP]
engineid=LE_v3Engine
defreadcomm=public
defwritecomm=private
deftrapcomm=public
authtrap=disable
com2sec_count=0
group_count=0
view_count=1
view1_name=all
view1_type=included
view1_subtree=.1
view1_mask=ff

--more—
...
```

FIGURE 5–3: Displaying specific modules using the 'show config' command

```
ML2400# show config module=snmp,system
[HARDWARE]
type= ML2400
slotB=8 Port TP Module
############################################################
# System Manager - This area configures System related     #
#          information.                                    #
############################################################
[SYSTEM]
***Edit below this line only****
system_name=Main
system_contact=someone@joe.com
system_location= Markham, Ontario
boot_mode=manual
system_ip=192.168.1.15
system_subnet=0.0.0.0
system_gateway=192.168.1.11
idle_timeout=10
telnet_access=enable
snmp_access=enable
web_access=enable

--more—
…
```

FIGURE 5–4: Displaying configuration for different modules.
Note – multiple modules can be specified on the command line

5.4.4 Saving Configuration

It is advisable to save the configuration before updating the software, as it may be necessary in certain situations. The `loadconf` command requires a reboot to activate the new configuration. Without a reboot, the ML2400 used the previous configuration. When reboot is selected, the user is prompted as follows:

```
Reboot? ['Y' or 'N']
```

Select "Y". The ML2400 will prompt:

```
Save Current Configuration?
```

Select "N".

Additional capabilities have been added to save and load configurations. The commands are:

ftp *<get|put|list|del> type=<app|config|oldconf|script|hosts|log> host=<hostname> ip=<ipaddress> file=<filename> user=<user> pass=<password>*

tftp *<get|put> type=<app|config|oldconf|script|hosts|log> host=<hostname> ip=<ipaddress> file=<filename>*

xmodem *<get|put> type=<app|config|oldconf|script|hosts|log>*

The arguments are describe below:

`type`: Specifies whether a log file or host file is uploaded or downloaded. This can also perform the task of exporting a configuration file or uploading a new image to the switch

`host`, `ip`, `file`, `user`, `pass`: These parameters are associated with ftp/tftp server communications.

The user can save the configuration in old (v2 format) and new (v3 format). The v3 format must be used to utilize the ASCII and CLI Script capability.

save *[format=v2|v3]*

With release 1.7 and higher, the configuration can be saved in the older format (binary object) or in a new format as an ASCII file. The new format is recommended by GE Multilin. Use the old format only if there are multiple MultiLink switches on the network running different versions of software. GE Multilin recommends upgrading all switches to the most current software release.

To ease the process of uploading and executing a series of commands, the ML2400 can create a host (equivalent to creating a host table on many systems). The command for creating a host is:

host *<add|edit|del> name=<host-name> ip=<ipaddress> user=<user> pass=<password>*

The `show host` command displays the host table entries

```
ML2400# access
ML2400(access)## host add name=server ip=192.168.5.2
Host added successfully
ML2400(access)## show host
No  Host Name  IP Address   User  Password
========================================
1   server     192.168.5.2  --    ******
2   --         --           --    --
3   --         --           --    --
4   --         --           --    --
5   --         --           --    --
6   --         --           --    --
7   --         --           --    --
8   --         --           --    --
9   --         --           --    --
10  --         --           --    --
ML2400(access)##
```

5.4.5 Script File

Script file is a file containing a set of CLI commands which are used to configure the switch. CLI commands are repeated in the file for clarity, providing guidance to the user editing the file as to what commands can be used for modifying variables used by MNS. The script file does not have a check sum at the end and is used for configuring a large number of switches easily. As with any configuration file that is uploaded, GE Multilin, Inc. recommends that modifications of this file and the commands should be verified by the user in a test environment prior to use in a "live" production network.

The script file will look familiar to people familiar with the CLI commands as all the commands saved in the script file are described in the CLI User Guide. A sample of the script file is shown below.

```
##################################################################
#
# Copyright (c) 2001-2005 GE Multilin, Inc All rights reserved.
# RESTRICTED RIGHTS
# --------------------------------
# Use, duplication or disclosure is subject to U.S. Government
# restrictions as set forth in Sub-division (b)(3)(ii) of the
# rights in Technical Data and Computer Software clause at
# 52.227-7013.
#
# This file is provided as a sample template to create a backup
# of GE MultiLink switches configurations. As such,
# this script provides insights into the configuration of GE MultiLink switch's settings.
# GE Multilin, Inc. recommends that modifications of this
# file and the commands should be verified by the User in a
# test environment prior to use in a "live" production network.
# All modifications are made at the User's own risk and are
# subject to the limitations of the GE MultiLink MNS End User
# License Agreement (EULA). Incorrect usage may result in
# network shutdown. GE Multilin, Inc. is not liable for incidental or
# consequential damages due to improper use.
##################################################################
#

############################################################
# System Manager - This area configures System related                #
#              information.                                          #
############################################################

set bootmode type=manual
ipconfig ip=192.168.5.5 mask=0.0.0.0 dgw=0.0.0.0
set timeout=10
access
telnet enable
snmp enable
web=enable
exit
############################################################
# User Accounts - This area configures user accounts for              #
#              accessing this system.                                #
############################################################

user
add user=manager level=2
passwd user=manager
manager
<additional lines deleted for succinct viewing>
```

In the above example, note that all the commands are CLI commands. This script provides an insight into the configuration of GE MultiLink switches settings. GE Multilin, Inc. recommends that modifications of this file and the commands should be verified by the User in a test environment prior to use in a "live" production network

To ease the process of uploading the script files, use the Script Upload/Download capability described above.

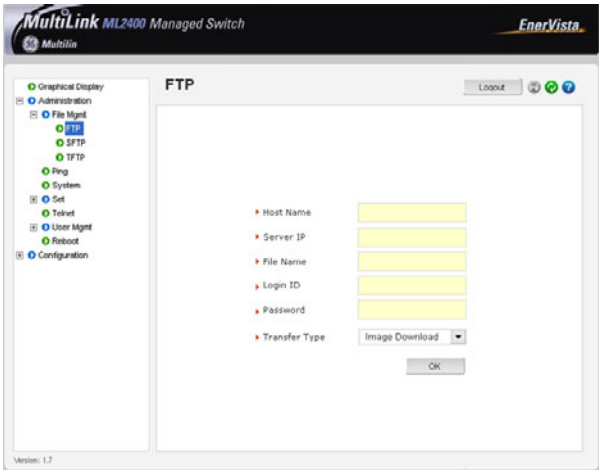
5.4.6 Saving and Loading – EnerVista Software

NOTE

Place the Switch offline while transferring Setting Files to the Switch.
When transferring Settings Files from one Switch to another, the IP address of the originating Switch will also be transferred. The user must therefore reset the IP address on the receiving Switch before connecting to the network.

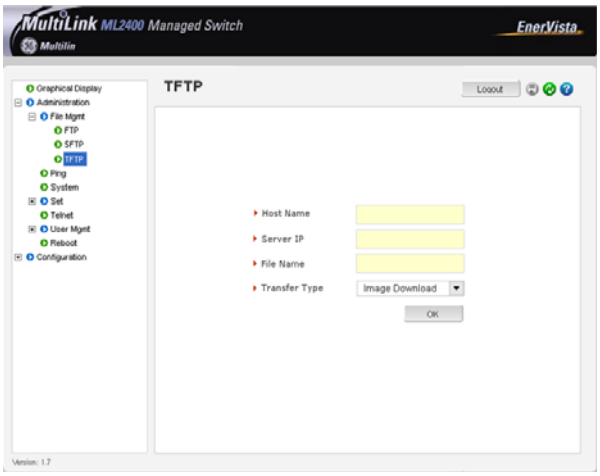
After configuration changes are made, all the changes are automatically saved. It is a good practice to save the configuration on another server on the network using the `tftp` or `ftp` protocols. Once the configuration is saved, the saved configuration can be reloaded to restore the settings. At this time, the saved or loaded configuration parameters are not in a human readable format.

The following figure illustrates the FTP window, which can be used to save the configuration, as well as up load new images or reload a saved configuration.



Ensure the machine specified by the IP address has the necessary services running on it. For serial connections, x-modem or other alternative methods can be used. Generally, the filename name must be a unique filename, as over-writing files is not permitted by most FTP and TFTP servers (or services).

The following figure illustrates saving the configuration on a TFTP server. Note that the menu is similar to the FTP screen described earlier.



This process can also be used to update new software to the managed MultiLink switches. Before the software is updated, it is advised to save the configurations. Reloading of the configuration is not usually necessary, but in certain situations it may be needed, and it is recommended that you save configurations before a software update. Make sure to reboot the switch after a new configuration is loaded.

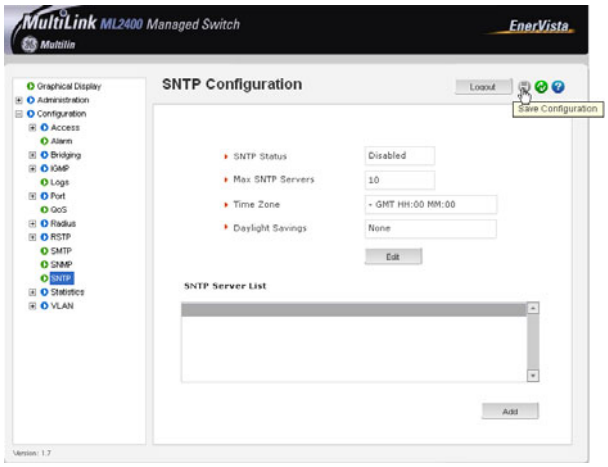
The file transfer operations allowed are:

1. Image Download (or Image Upload): Copy the ML2400 image from switch to the server (or from the server to the switch). The "Image Upload" option is commonly used to upgrade the ML2400 image on the switch.
2. Config Download (or Config Upload): Save the configuration of the switch on the server (or load the saved configuration from the server to the switch). This option is used to save a backup of the ML2400 configuration or restore the configuration (in case of a disaster.)
3. Script Download (or Script Upload): Save the necessary CLI commands used for configuration of the switch (or upload the necessary CLI commands needed to configure the switch). This option is used to ease the repetitive task of configuring multiple commands or reviewing all the commands needed to configure the ML2400.
4. Host Download (or Host Upload): Save the host information. The hosts are created by the Configuration - Access - Host commands
5. Log Upload - Save the log file on the ftp/tftp server

To save any changes,

- ▷ **Click on the save ( ) icon.**
  The software will ask again if the changes need to be saved or ignored.
- ▷ **If the changes need to be ignored, click on Cancel and reboot the switch.**
- ▷ **If the changes need to be saved, click on OK.**

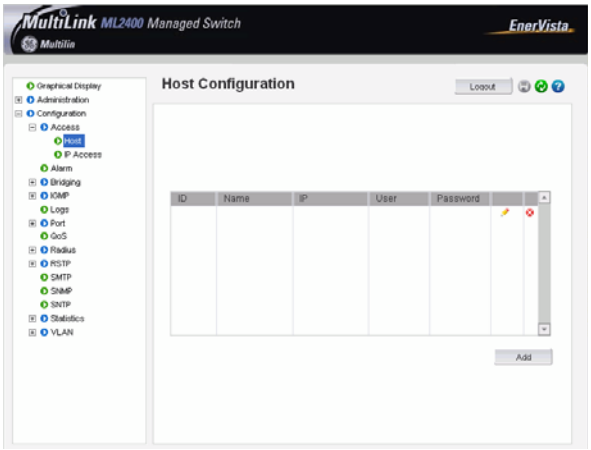
The following figures illustrate saving changes made after adding an SNTP server. This is done by clicking on the **Save** icon to save current configuration



5.4.7 Host Names

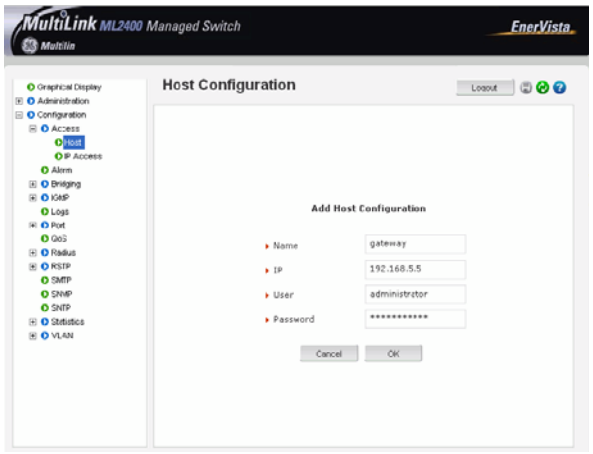
Instead of typing in IP addresses of commonly reached hosts, the ML2400 allows hosts to be created with the necessary host names, IP addresses, user names, and passwords.

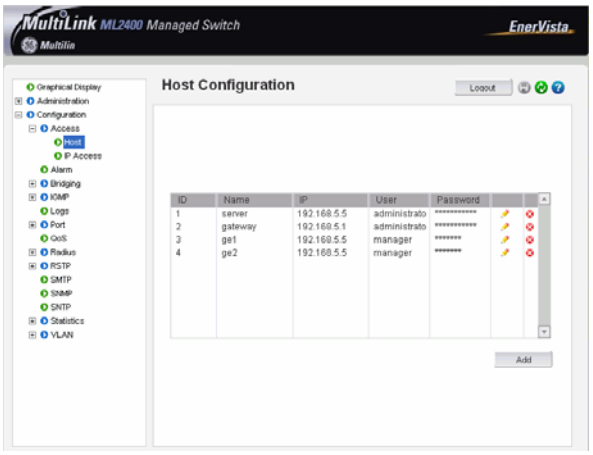
▷ Use the **Configuration > Access > Host** menu to create host entries as shown below.



▷ To add a host, click the **Add** button.

▷ Fill in all the fields below to create the necessary host entries.





▷ To delete or edit the entries, use the delete or edit icons next to each entry shown above.

5.4.8 Erasing Configuration

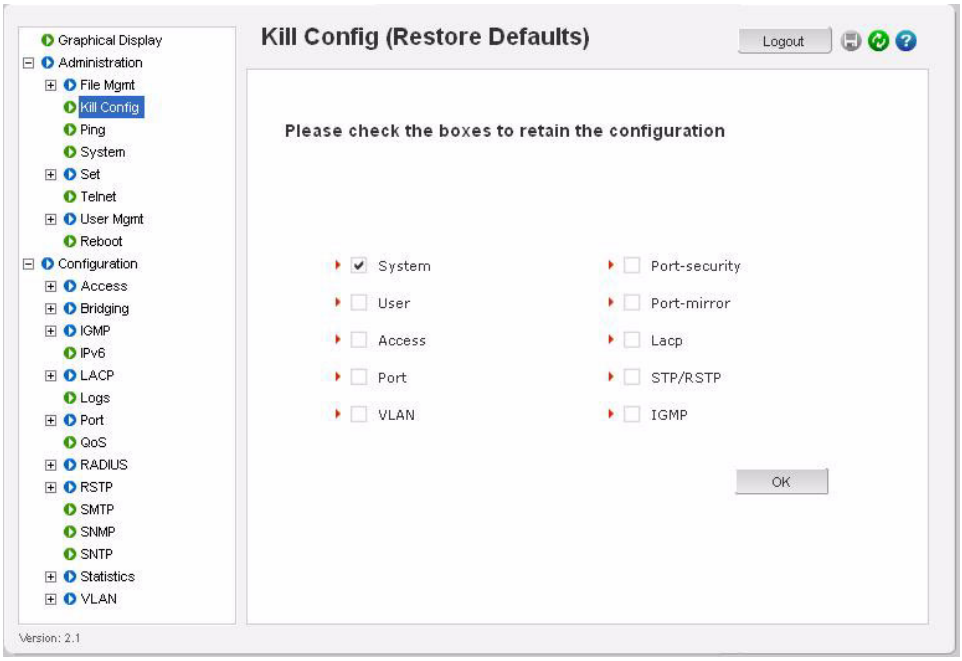
Kill Config option using SWM

To erase the configuration and reset the configurations to factory defaults, you can use the *kill config* option from Administration tab by selecting **kill config**.

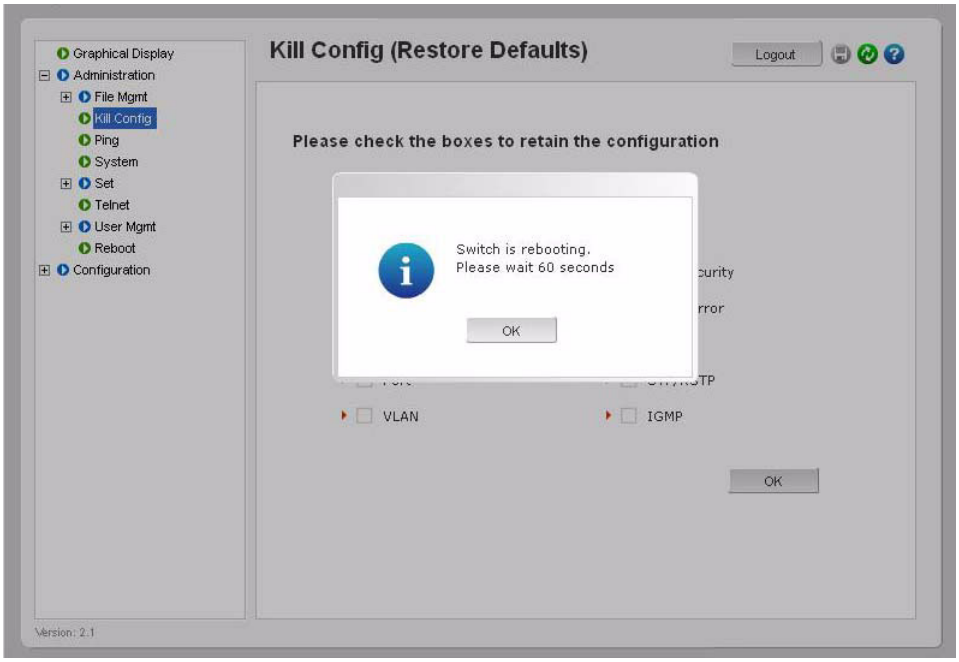
NOTE

User also has the option to save one module from defaulting back to factory defaults by checking the module box before issuing kill Config command.

In the example below "system" module box has been checked. In this case after kill Config command is issued by pressing the **OK** button, the Switch will perform a factory dump restoring all the Switch settings back to factory defaults except for the "System" settings which will be retained.



When the **OK** button is pressed the Switch will issue the following warning messages; and reboot the switch for it to revert back to the factory default settings with the exceptions of modules opted not to be defaulted.



Here is a list of the modules and related settings that can be selected not to default back to factory default settings.

Name	Areas affected
System	IP Configuration, Boot mode
User	Users settings (e.g. login names, passwords)
Port	Port settings, Broadcast Protection and QoS settings
STP/RSTP	STP, RSTP settings
Port-Security	Port Security settings
Port-Mirror	Port Mirror settings
VLAN	Port/Tag VLAN settings
ACCESS	IP-Access and Host Table settings
IGMP	IGMP Settings
LACP	LACP settings

Kill Config option using CLI

This command is a “hidden command”; that is, the on-line help and other help functions normally do not display this command. The syntax for this command is:

kill Config

or

kill config save=module command

The *kill Config* command will default all the Switch settings back to factory defaults, while the *kill config save=module* will default all with the exception of module selected.

Available modules are: system, user, acces, port, vlan, ps, mirror, lacp, slp, and igmp.

It is recommended to save the configuration (using saveconf command discussed above) before using the kill config command. The following two examples illustrate how to erase all the Switch's configuration using the kill config command and the second example illustrates how to erase all the Switch's configuration with the exception of 'system' configuration.

ML2400# kill config

```
Do you want to erase the configuration?
['Y' or 'N'] Y
Successfully erased configuration...Please reboot.
```

ML2400# kill config save=system

```
Do you want to erase the configuration?
['Y' or 'N'] Y
Successfully erased configuration...Please reboot.
```

Once the configuration is erased, please reboot the switch for the changes to take effect.

5.5 IPv6

This section explains how to access the GE MultiLink switches using IPv6 instead of IPv4 addressing. IPv6 provides a much larger address space and its use is often required.

Assumptions

It is assumed here that the user is familiar with IP addressing schemes and has other supplemental material on IPv6, configuration, routing, setup and other items related to IPv6. This user guide does not discuss these details.

5.5.1 Introduction to IPv6

IPv6 is short for "Internet Protocol Version 6". IPv6 is the "next generation" protocol or IPng and was recommended to the IETF to replace the current version Internet Protocol, IP Version 4 ("IPv4"). IPv6 was recommended by the IPv6 (or IPng) Area Directors of the Internet Engineering Task Force at the Toronto IETF meeting on July 25, 1994 in RFC 1752: The Recommendation for the IP Next Generation Protocol. The recommendation in question, was approved by the Internet Engineering Steering Group and a proposed standard was created on November 17, 1994. The core set of IPv6 protocols was created as an IETF draft standard on August 10, 1998.

IPv6 is a new version of IP, designed to be an evolutionary step from IPv4. It is a natural increment to IPv4. It can be installed as a normal software upgrade in internet devices and is interoperable with the current IPv4. Its deployment strategy is designed to have no dependencies. IPv6 is designed to run well on high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and at the same time still be efficient on low bandwidth networks (e.g. wireless). In addition, it provides a platform for the new level of internet functionality that will be required in the near future.

IPv6 includes a transition mechanism designed to allow users to adopt and deploy it in a highly diffuse fashion, and to provide direct interoperability between IPv4 and IPv6 hosts. The transition to a new version of the Internet Protocol is normally incremental, with few or no critical interdependencies. Most of today's internet uses IPv4, which is now nearly twenty years old. IPv4 has been remarkably resilient in spite of its age, but it is beginning to have problems. Most importantly, there is a growing shortage of IPv4 addresses, which are needed by all new machines added to the Internet.

IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses. It also adds many improvements to IPv4 in areas such as routing and network auto configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during the transition period.

5.5.2 What's changed in IPV6?

The changes from IPv4 to IPv6 fall primarily into the following categories:

- Expanded Routing and Addressing Capabilities – IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of

addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses.

- A new type of address called an "anycast address" is defined, that identifies sets of nodes where a packet sent to an anycast address is delivered to one of these nodes. The use of anycast addresses in the IPv6 source route allows nodes to control the path along which their traffic flows.
- Header Format Simplification - Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to keep the bandwidth cost of the IPv6 header as low as possible despite the increased size of the addresses. Even though the IPv6 addresses are four times longer than the IPv4 addresses, the IPv6 header is only twice the size of the IPv4 header.
- Improved Support for Options - Changes in the way IP header options are encoded allow more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.
- Quality-of-Service Capabilities - A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real- time" service.
- Authentication and Privacy Capabilities - IPv6 includes the definition of extensions which provide support for authentication, data integrity, and confidentiality. This is included as a basic element of IPv6 and will be included in all implementations.

5.5.3 IPv6 Addressing

IPv6 addresses are 128-bits long and are identifiers for individual interfaces and sets of interfaces. IPv6 addresses of all types are assigned to interfaces, not nodes. Since each interface belongs to a single node, any of that node's interface's unicast addresses may be used as an identifier for the node. A single interface may be assigned multiple IPv6 addresses of any type.

There are three types of IPv6 addresses. These are unicast, anycast, and multicast. Unicast addresses identify a single interface. Anycast addresses identify a set of interfaces such that a packet sent to an anycast address will be delivered to one member of the set. Multicast addresses identify a group of interfaces, such that a packet sent to a multicast address is delivered to all the interfaces in the group. There are no broadcast addresses in IPv6. This function has been replaced by multicast addresses.

IPv6 supports addresses which are four times the number of bits as IPv4 addresses (128 vs. 32). This is 4 Billion x 4 Billion x 4 Billion (296) times the size of the IPv4 address space (232). This works out to be:

340,282,366,920,938,463,463,374,607,431,768,211,456

This is an extremely large address space. In a theoretical sense this is approximately 665,570,793,348,866,943,898,599 addresses per square meter of the surface of the planet Earth (assuming the earth surface is 511,263,971,197,990 square meters). In the most pessimistic estimate this would provide 1,564 addresses for each square meter of the surface of Earth. The optimistic estimate would allow for 3,911,873,538,269,506,102 addresses for each square meter of the surface Earth. Approximately fifteen percent of the address space is initially allocated. The remaining 85% is reserved for future use.

Details of the addressing are covered by numerous articles on the WWW as well as other literature, and are not covered here.

5.5.4 Configuring IPv6

The commands used for IPv6 are the same as those used for IPv4. Some of the commands will be discussed in more details later. The only exception is the 'ping' command where there is a special command for IPv6. That commands is 'ping6' and the syntax is as

Syntax **ping6 <IPv6 address>** - *pings an IPv6 station.*

There is also a special command to ping the status of IPv6. That command is

Syntax **show ipv6** - *displays the IPv6 information.*

To configure IPv6, the following sequence of commands can be used:

```
ML2400# ipconfig ?
ipconfig :  Configures the system IP address, subnet mask and gateway
Usage
ipconfig [ip=<ipaddress>] [mask=<subnet-mask>] [dgw=<gateway>]

ML2400# ipconfig ip=fe80::220:6ff:fe25:ed80 mask=ffff:ffff:ffff:ffff::
 Action Parameter Missing. "add" assumed.
 IPv6 Parameters Set.
ML2400# show ipv6

 IPv6 Address : fe80::220:6ff:fe25:ed80 mask : ffff:ffff:ffff:ffff::

ML2400# show ipconfig
 IP Address :  192.168.5.5
 Subnet Mask:  255.255.255.0
 Gateway Address:  192.168.5.1
 IPv6 Address:  fe80::220:6ff:fe25:ed80 mask : ffff:ffff:ffff:ffff::
 IPv6 Gateway:  ::

ML2400#
```

FIGURE 5–5: Configuring IPv6

In addition to the commands listed above, the commands which support IPv6 addressing are

Syntax **ftp <IPv6 address>** - *ftp to an IPv6 station*

Example – **ftp fe80::220:6ff:fe25:ed80**

Syntax **telnet <IPv6 address>** *- telnet to an IPv6 station*

Example – **telnet fe80::220:6ff:fe25:ed80**

Besides, if the end station supports IPv6 addressing (as most Linux and Windows systems do), one can access the switch using the IPv6 addressing as shown in the example below

http://fe80::220:6ff:fe25:ed80

5.5.5 List of commands in this chapter

Syntax **ipconfig [ip=<ip-address>] [mask=<subnet-mask>] [dgw=<gateway>] [add|del]** *– configure an IPv6 address. The add/delete option can be used to add or delete IPv4/IPv6 addresses.*

Syntax **show ipconfig** *– display the IP configuration information – including IPv6 address*

Syntax **ping6 <IPv6 address>** *- pings an IPv6 station*

Syntax **show ipv6** *- displays the IPv6 information*

Syntax **ftp <IPv6 address>** *- ftp to an IPv6 station*

Syntax **telnet <IPv6 address>** *- telnet to an IPv6 station.*

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 6: Access Considerations

6.1 Securing Access

6.1.1 Description

This section explains how the access to the MultiLink family of switches can be secured. Further security considerations are also covered such as securing access by IP address or MAC address.

It is assumed here that the user is familiar with issues concerning security as well as securing access for users and computers on a network. Secure access on a network can be provided by authenticating against an allowed MAC address as well as IP address.

6.1.2 Passwords

The GE MultiLink family of switches have a factory default password for the manager as well as the operator account. Passwords can be changed from the user ID by using the `set password` command.

For example:

```
ML2400# set password
Enter Current Password: *******
Enter New Password:*******
Confirm New Password:*******
Password has been modified successfully
ML2400#
```

Other details on managing users and the passwords are covered in *User Management* on page 1–14.

6.1.3 Port Security Feature

The port security feature can be used to block computers from accessing the network by requiring the port to validate the MAC address against a known list of MAC addresses. This port security feature is provided on an Ethernet, Fast Ethernet, or Gigabit Ethernet port. In case of a security violation, the port can be configured to go into the disable mode or drop mode. The disable mode disables the port, not allowing any traffic to pass through. The drop mode allows the port to remain enabled during a security violation and drop only packets that are coming in from insecure hosts. This is useful when there are other network devices connected to the MultiLink family of switches. If there is an insecure access on the secondary device, the MultiLink family of switches allow the authorized users to continue to access the network; the unauthorized packets are dropped preventing access to the network.

Network security hinges on the ability to allow or deny access to network resources. This aspect of secure network services involves allowing or disallowing traffic based on information contained in packets, such as the IP address or MAC address. Planning for access is a key architecture and design consideration. For example, which ports are configured for port security? Normally rooms with public access (e.g. lobby, conference rooms, etc.) should be configured with port security. Once that is decided, the next few decisions are: Who are the authorized and unauthorized users? What action should be taken against authorized as well as unauthorized users? How are the users identified as authorized or unauthorized?

6.2 Configuring Port Security through the Command Line Interface

6.2.1 Commands

To configure port security, login as a level 2 user or as a manager. Once logged in, get to the port-security configuration level to setup and configure port security with the following command syntax:

configure port-security
port-security

For example, using the `configure port-security` command:

ML2400# `configure port-security`

ML2400(port-security)##

Alternately, the `port-security` command can also be used to enter the port-security configuration mode:

ML2400# `port-security`

ML2400#(port-security)##

From the port security configuration mode, the switch can be configured to:

1. Auto-learn the MAC addresses.
2. Specify individual MAC addresses to allow access to the network.
3. Validate or change the settings.

The command syntax for the above actions are:

allow *mac=<address|list|range>*
port=<num|list|range>
learn *port=<number-list> <enable|disable>*
show port-security
action *port=<num|list|range>*
<none|disable|drop>
signal *port=<num|list|range>*
<none|log|trap|logandtrap>
ps *<enable|disable>*
remove *mac=<all|address|list|range>*
port=<num|list|range>
signal *port=<num|list|range>*
<none|log|trap|logandtrap>

Where the following hold:

- `allow mac` - configures the switch to setup allowed MAC addresses on specific ports
- `learn port` - configures the switch to learn the MAC addresses associated with specific port or a group of ports
- `show port-security` - shows the information on port security programmed or learnt
- `action port` - specifies the designated action to take in case of a non authorized access
- `ps` - port security - allows port security to be enable or disabled

- `remove mac` - removes specific or all MAC addresses from port security lookup
- `signal port=<num|list|range>` - observe list of specified ports and notify if there is a security breach on the list of port specified. The signal can be a log entry, a trap to the trap receiver specified as part of the SNMP commands (where is that specified) or both

There is a limitation of 200 MAC addresses per port and 500 MAC addresses per switch for port security.

All commands listed above must be executed under the port security configuration mode.

Let's look at a few examples. The following command allows specific MAC addresses on a specified port. No spaces are allowed between specified MAC addresses.

```
ML2400(port-security)## allow
mac=00:c1:00:7f:ec:00,00:60:b0:88:9e:00 port=18
```

The following command sequence sets the port security to learn the MAC addresses. Note that a maximum of 200 MAC addresses can be learned per port, to a maximum of 500 per switch. Also, the `action` on the port must be set to none before the port learns the MAC address information.

```
ML2400(port-security)## action port=9,10 none
ML2400(port-security)## learn port=9,10 enable
```

The following command sequence enables and disables port security

```
ML2400(port-security)## ps enable
  Port Security is already enabled
ML2400(port-security)## ps disable
  Port Security Disabled
ML2400 ps enable
  Port Security Enabled
```

Example 6-1 views port security settings on a switch. Learning is enabled on port 9. This port has 6 stations connected to it with the MAC addresses as shown. Other ports have learning disabled and the MAC addresses are not configured on those ports.

Example 6-2 shows how to enable learning on a port. After the learning is enabled, the port security can be queried to find the status of MAC addresses learnt. If there were machines connected to this port, the MAC address would be shown on port 11 as they are shown on port 9.

Example 6-1: Viewing the port security settings

```
ML2400# show port-security
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 9    ENABLE  LOG     NONE    ENABLE    6    00:e0:29:2a:f1:bd
                                              00:01:03:e2:27:89
                                              00:07:50:ef:31:40
                                              00:e0:29:22:15:85
                                              00:03:47:ca:ac:45
                                              00:30:48:70:71:23
 10   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 11   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 12   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 13   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 14   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 15   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 16   ENABLE  NONE    NONE    DISABLE   0    Not Configured
ML2400(port-security)##
```

Example 6-2: Enabling learning on a port

```
ML2400(port-security)## learn port=11 enable
  Port Learning Enabled on selected port(s)
ML2400(port-security)## show port-security
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 9    ENABLE  LOG     NONE    ENABLE    6    00:e0:29:2a:f1:bd
                                              00:01:03:e2:27:89
                                              00:07:50:ef:31:40
                                              00:e0:29:22:15:85
                                              00:03:47:ca:ac:45
                                              00:30:48:70:71:23
 10   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 11   ENABLE  NONE    NONE    ENABLE    0    Not Configured
 12   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 13   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 14   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 15   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 16   ENABLE  NONE    NONE    DISABLE   0    Not Configured
ML2400(port-security)##
```

Example 6-3 shows how to allow specific MAC address on specific ports. After the MAC address is specified, the port or specific ports or a range of ports can be queried as shown.

Example 6-4 shows how to remove a MAC address from port security

To set logging on a port, use the following command sequence:

```
ML2400(port-security)## signal port=11 logandtrap
  Port security Signal type set to Log and
  Trap on selected port(s)
```

The examples provided illustrate the necessary commands to setup port security. The recommended steps to setup security are:

- Set the ML2400 software to allow port security commands (use the `port-security` command).
- Enable port security (use the `enable ps` command).
- Enable learning on the required ports (for example, use the `learn port=11` enable command for port 11).
- Verify learning is enables and MAC addresses are being learnt on required ports (use the `show port-security port=11` command).
- Save the port-security configuration (use the `save` command).
- Disable learning on required ports (for example, use the `learn port=11,15 disable` command).

Example 6-3: Allowing specific MAC addresses on specific ports

```
ML2400(port-security)## allow mac=00:c1:00:7f:ec:00 port=9,11,13
  Specified MAC address(es) allowed on selected port(s)
ML2400(port-security)## show port-security port=9,11,13
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 9    ENABLE  LOG     NONE    ENABLE    6    00:e0:29:2a:f1:bd
                                             00:01:03:e2:27:89
                                             00:07:50:ef:31:40
                                             00:e0:29:22:15:85
                                             00:03:47:ca:ac:45
                                             00:30:48:70:71:23
                                             00:c1:00:7f:ec:00
 11   ENABLE  NONE    NONE    ENABLE    0    00:c1:00:7f:ec:00
 13   ENABLE  NONE    NONE    DISABLE   0    00:c1:00:7f:ec:00
```

Example 6-4: Removing MAC addresses from specific ports

```
ML2400(port-security)## remove mac=00:c1:00:7f:ec:00 port=13
 Specified MAC address(es) removedfrom selected
  port(s)
ML2400(port-security)## show port-security port=13
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 13   ENABLE  NONE    NONE    ENABLE    0    Not Configured
ML2400(port-security)##
```

- ▷ (Optional step) Add any specific MAC addresses, if needed, to allow designated devices to access the network (use the `add mac=00:c1:00:7f:ec:00 port=11,15` command).
- ▷ Disable access to the network for unauthorized devices (Use `action port=11 <diable|drop>` depending on whether the port should be disabled or the packed dropped. Follow that with a `show port-security` command to verify the setting).
- ▷ (Optional step) Set the notification to notify the management station on security breach attempts (use the command `signal port` to make a log entry or send a trap).

Example 6-5 illustrates these steps for setting up port security on a specific port:

Once port security is setup, it is important to manage the log and review the log often. If the signals are sent to the trap receiver, the traps should also be reviewed for intrusion and other infractions.

6.2.2 Security Logs

All events occurring on the MultiLink family of switches are logged. The events can be informational (e.g. login, STP synchronization etc.), debugging logs (for debugging network and other values), critical (critical events), activity (traffic activity) and fatal events (such as

Example 6-5: Configuring port security

```
ML2400# port-security
ML2400(port-security)## ps enable
  Port Security is already enabled
ML2400(port-security)## learn port=11 enable
  Port Learning Enabled on selected port(s)
ML2400(port-security)## show port-security
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 9    ENABLE  LOG     NONE    ENABLE    6    00:e0:29:2a:f1:bd
                                             00:01:03:e2:27:89
                                             00:07:50:ef:31:40
                                             00:e0:29:22:15:85
                                             00:03:47:ca:ac:45
                                             00:30:48:70:71:23
 10   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 11   ENABLE  NONE    NONE    ENABLE    0    00:c1:00:7f:ec:00
 12   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 13   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 14   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 15   ENABLE  NONE    NONE    DISABLE   0    Not Configured
 16   ENABLE  NONE    NONE    DISABLE   0    Not Configured
ML2400(port-security)## save
  Saving current configuration
  Configuration saved
ML2400(port-security)## learn port=11 disable
  Port Learning Disabled on selected port(s)
ML2400(port-security)## action port=11 drop
  Port security Action type set to Drop on selected
  port(s)
ML2400(port-security)## show port-security port=11
PORT  STATE   SIGNAL  ACTION  LEARN   COUNT  MAC ADDRESS
----  -----   ------  ------  -----   -----  -----------
 11   ENABLE  NONE    DROP    ENABLE    0    00:c1:00:7f:ec:00
ML2400(port-security)## signal port=11 logandtrap
  Port security Signal type set to Log and Trap on
  selected port(s)
ML2400(port-security)## exit
ML2400#
```

unexpected behavior). The specific types of logs can be viewed and cleared. The `show log` command displays the log information and the `clear log` command clears the log entries. The syntax for these commands is shown below:

show log *[1..5|informational|debug|fatal |critical|activity]*
clear log *[informational|debug|activity |critical|fatal]*

The `set logsize` command set the number of lines to be collected in the log before the oldest record is re-written. The syntax for this command is:

set logsize *size=<1-1000>*

Example 6-6 illustrates the `show log` and `clear log` commands. The `show log` command indicates the type of log activity in the S column. I indicates informational entries and A indicates activities which are a result of port-security setup. Notice the `clear log informational` command clears the informational entries only.

The log shows the most recent intrusion at the top of the listing. If the log is filled when the switch detects a new intrusion, the oldest entry is dropped off the listing.

As discussed in the prior section, any port can be set to monitor security as well as make a log on the intrusions that take place. The logs for the intrusions are stored on the switch. When the switch detects an intrusion on a port, it sets an "alert flag" for that port and makes the intrusion information available.

The default log size is 50 rows. To change the log size, use the `set logsize` command.

Example 6-6: Security log commands

```
ML2400# show log
S  Date        Time          Log Description
-  ----        ----          ---------------
I  12-07-2004  9:01:34 A.M   CLI:manager console login
I  12-07-2004  5:54:23 P.M   SNTP:Date and Time updated from SNTP server
I  12-08-2004  6:09:00 P.M   SNTP:Date and Time updated from SNTP server
I  12-09-2004  1:48:56 P.M   TELNET:Telnet Session Started
I  12-09-2004  1:49:23 P.M   CLI:manager console login
I  12-09-2004  4:26:26 P.M   TELNET:Telnet Session Started
I  12-09-2004  4:26:34 P.M   CLI:manager console login
I  12-09-2004  6:23:37 P.M   SNTP:Date and Time updated from SNTP server
I  12-10-2004  6:38:13 P.M   SNTP:Date and Time updated from SNTP server
I  12-11-2004  10:16:24 A.M  TELNET:Telnet Session Started
I  12-11-2004  6:52:49 P.M   SNTP:Date and Time updated from SNTP server
I  12-12-2004  12:40:35 P.M  TELNET:Telnet Session Started
I  12-12-2004  12:40:42 P.M  CLI:manager console login
A  12-17-2004  12:05:52 P.M  PS:INTRUDER 00:e0:29:6c:a4: fd@port11, packet dropped
A  12-17-2004  12:07:04 P.M  PS:INTRUDER 00:50:0f:02:33: b6@port15, packet dropped
A  12-17-2004  12:07:16 P.M  PS:INTRUDER 00:e0:29:2a:f0: 3a@port15, packet dropped
ML2400# clear log informational
  Clear Logged Events? ['Y' or 'N']
ML2400# show log
S  Date        Time          Log Description
-  ----        ----          ---------------
A  12-17-2004  12:05:52 P.M  PS:INTRUDER 00:e0:29:6c:a4: fd@port11, packet dropped
A  12-17-2004  12:07:04 P.M  PS:INTRUDER 00:50:0f:02:33: b6@port15, packet dropped
A  12-17-2004  12:07:16 P.M  PS:INTRUDER 00:e0:29:2a:f0: 3a@port15, packet dropped
```

When the switch detects an intrusion attempt on a port, it records the date and time stamp, the MAC address, the port on which the access was attempted and the action taken by ML2400 software. The event log lists the most recently detected security violation attempts. This provides a chronological entry of all intrusions attempted on a specific port.

The event log records events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each event log entry is composed of four fields

- **Severity** - the level of severity (see below).
- **Date** - date the event occurred on. See *Date and Time* on page 5–9 for information on setting the date and time on the switch.
- **Time** - time the event occurred on. See *Date and Time* on page 5–9 for information on setting the date and time on the switch
- **Log Description** - description of event as detected by the switch

Severity has one of the following values, and depending on the severity type, is assigned a severity level.

- `I` (information, severity level 1) indicates routine events.
- `A` (activity, severity level 2) indicates the activity on the switch.
- `D` (debug, severity level 3) is reserved for GE Multilin internal diagnostic information
- `C` (critical, severity level 4) indicates that a severe switch error has occurred.
- `F` (fatal, severity level 5) indicates that a service has behaved unexpectedly.

6.2.3 Authorized Managers

Just as port security allows and disallows specific MAC addresses from accessing a network, the ML2400 software can allow or block specific IP addresses or a range of IP addresses to access the switch. The `access` command allows access to configuration mode:

access

The `allow ip` command allows specified services for specified IP addresses. IP addresses can be individual stations, a group of stations or subnets. The range is determined by the IP address and netmask settings.

allow *ip=<ipaddress> mask=<netmask> service=<name|list>*

The `deny ip` command denies access to a specific IP address(es) or a subnet. IP addresses can be individual stations, a group of stations or subnets. The range is determined by the IP address and netmask settings.

deny *ip=<ipaddress> mask=<netmask> service=<name|list>*

The `remove ip` command removes specific IP address(es) or subnet by eliminating specified entry from the authorized manager list.

remove *ip=<ipaddress> mask=<netmask>*

The `removeall` command removes all authorized managers.

removeall

The `show ip-access` command displays a list of authorized managers

show ip-access

NOTE

It is assumed here that the user is familiar with IP addressing schemes (e.g. class A, B, C, etc.), subnet masking and masking issues such as how many stations are allowed for a given subnet mask.

In Example 6-7, any computer on 3.94.245.10 network is allowed (note how the subnet mask indicates this). Also, a specific station with IP address 3.94.245.25 is allowed (again note how the subnet mask is used). An older station with IP address 3.94.245.15 is removed.

Example 6-7: Allowing/blocking specific IP addresses

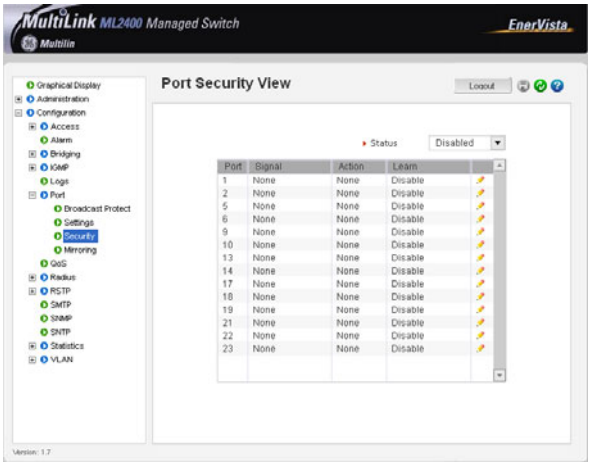
```
ML2400# access
ML2400(access)## allow ip=3.94.245.10 mask=255.255.255.0 service=t
  Service(s) allowed for specified address
ML2400(access)## allow ip=3.94.245.25 mask=255.255.255.255 service
  Service(s) allowed for specified address
ML2400(access)## remove ip=3.94.245.15 mask=255.255.255.255
  Access entry removed
ML2400(access)## exit
ML2400# show ip-access
    ============================================================
    IP Address      | Mask            | Telnet   | Web     | SNMP |
    ============================================================
    3.94.245.10       255.255.255.0     ALLOWED   DENIED   DENIED
    3.94.245.25       255.255.255.255   ALLOWED   DENIED   DENIED
```

6.3 Configuring Port Security with EnerVista Software

6.3.1 Commands

After enabling the EnerVista Secure Web Management software,

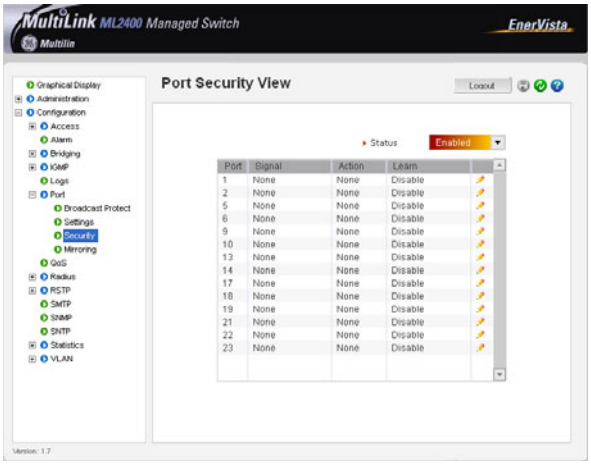
▷ Select the **Configuration > Port > Security** menu item to configure port security as shown below.



From the menu shown above, each individual port can be configured for the proper action on the port, auto learn MAC addresses and specify individual MAC addresses.

▷ To edit each port, click on the edit icon ( ).

▷ To enable or disable port security, use the **Status** drop down menu as shown below.



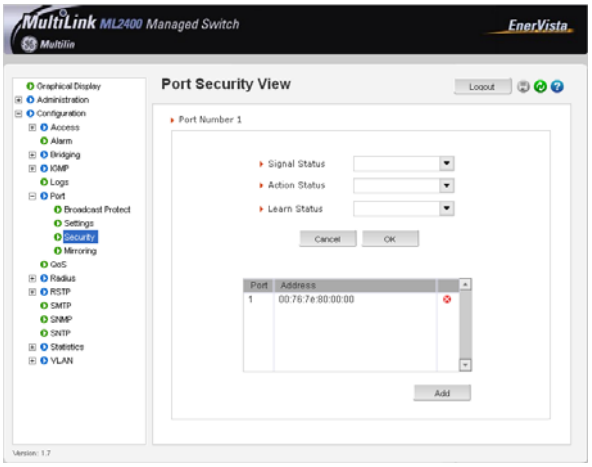
Note that the screen also provides an overview of each port on the switch. Each port can be individually configured for the proper port security action.

Each individual port can be configured by clicking on the edit icon ( ). Once the edit screen is shown, the following actions can be taken for each port:

1. The port can be specified to create a log entry or send a trap, do both or do nothing. This is done through the **Signal Status** drop down menu.
2. The port can be specified to drop the connection, disable the port or do nothing. This is indicated by the **Action Status** drop down menu.
3. The port can be put in the learn mode or the learning can be disabled. This is indicated by the **Learn Status** drop down menu.

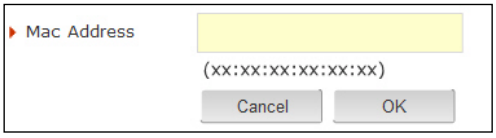
Additionally, MAC addresses can be added or deleted from the table of allowed MAC addresses.

- ▷ **To delete a MAC address, click on the delete icon ( ).**
- ▷ **To add a MAC address, click on the Add button and fill in the MAC address in the MAC address window.**



There is a limitation of 200 MAC addresses per port and 500 MAC addresses per switch for port security.

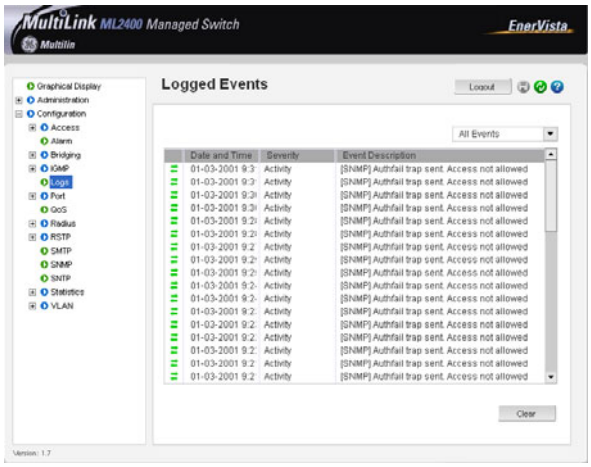
After clicking on the **Add** button, the following screen appears, allowing the entry of a specific MAC address



Once port security is setup, it is important to manage the log and review it often. If the signals are sent to the trap receiver, the traps should also be reviewed for intrusion and other infractions.

6.3.2 Logs

All events occurring on the Managed MultiLink switch are logged. The events can be informational (e.g. login, STP synchronization etc.), debugging logs (for debugging network and other values), critical (critical events), activity (traffic activity) and fatal events (such as unexpected behavior). The specific types of logs can be viewed and cleared. To view the logs in the EnerVista Secure Web Management software, select the **Configuration > Logs** menu item.



Note the different types of logs. Specific logs may be viewed by using the drop down menu in the top right corner

As discussed in the previous section, any port can be set to monitor security as well as make a log on the intrusions that take place. The logs for the intrusions are stored on the switch. When the switch detects an intrusion on a port, it sets an “alert flag” for that port and makes the intrusion information available.

NOTE

The default log size is 50 rows. To change the log size, select the **Configuration > Statistics > Log Statistics** menu item.

When the switch detects an intrusion attempt on a port, it records the date and time stamp, the MAC address, the port on which the access was attempted and the action taken by the MultiLink switches. The event log lists the most recently detected security violation attempts. This provides a chronological entry of all intrusions attempted on a specific port.

The event log records events as single-line entries listed in chronological order, and serves as a tool for isolating problems. Each event log entry is composed of four fields

- **Severity** - the level of severity (see below).
- **Date** - date the event occurred on. See *Date and Time* on page 5–8 for information on setting the date and time on the switch.
- **Time** - time the event occurred on. See *Date and Time* on page 5–8 for information on setting the date and time on the switch
- **Log Description** - description of event as detected by the switch

Severity has one of the following values, and depending on the severity type, is assigned a severity level.

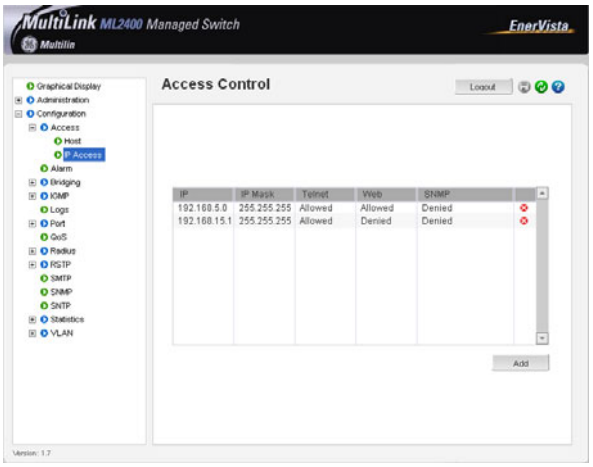
- `I` (information, severity level 1) indicates routine events.
- `A` (activity, severity level 2) indicates the activity on the switch.
- `D` (debug, severity level 3) is reserved for GE Multilin internal diagnostic information
- `C` (critical, severity level 4) indicates that a severe switch error has occurred.

- F (fatal, severity level 5) indicates that a service has behaved unexpectedly.

6.3.3 Authorized Managers

Just as port security allows and disallows specific MAC addresses from accessing a network, the EnerVista Secure Web Management software can allow or block specific IP addresses or a range of IP addresses to access the switch.

▷ Access this functionality via the **Configuration > Access > IP Access** menu item.

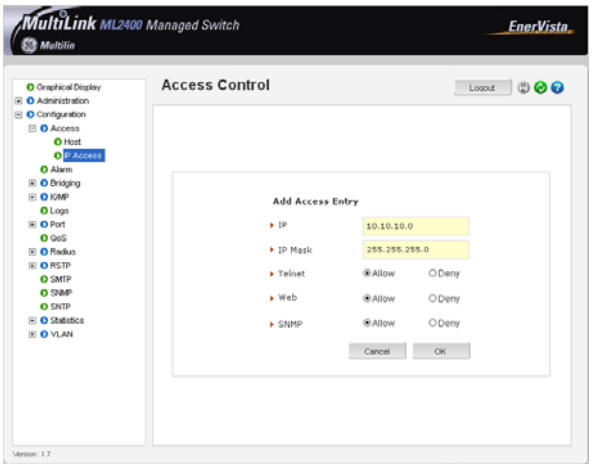


The window above show the authorized access list for managing the switch. Note specific services can be authorized. Also note that individual stations or a group of stations with IP addresses can be authorized.

NOTE

It is assumed that users are familiar with IP addressing schemes (e.g. class A, B, C etc.), subnet masking and masking issues such as how many stations are allowed for a given subnet mask.

In the following example, any computer on 10.10.10.0 sub network is allowed (note how the subnet mask is used to indicate that). Also, a specific station with IP address 192.168.15.25 is allowed (again note how the subnet mask is used to allow only one specific station in the network) and an older station with IP address 192.168.15.15 is removed.


MultiLink ML2400 Managed Switch
EnerVista
Multilin
Graphical Display
Administration
Configuration
Access
Host
IP Access
Alarm
Bridging
IGMP
Logs
Port
QoS
Radius
RSTP
SMTP
SNMP
SNTP
Statistics
VLAN
Access Control
Logout
Add Access Entry
IP
10.10.10.0
IP Mask
255.255.255.0
Telnet
Allow
Deny
Web
Allow
Deny
SNMP
Allow
Deny
Cancel
OK

Multilink ML2400

Ethernet Communications Switch

Chapter 7: Access Using RADIUS

7.1 Introduction to 802.1x

7.1.1 Description

The TACACS+ protocol is the latest generation of TACACS. TACACS is a simple UDP (User Datagram Protocol) based access control protocol originally developed by BBN for the MILNET (Military Network). Later the enhancements were called TACACS+. TACACS+ is a TCP (Transmission Control Protocol) based access control protocol. TCP offers a connection-oriented transport, while UDP offers best-effort delivery making the access authentication reliable.

Remote Authentication Dial-In User Service or RADIUS is a server that has been traditionally used by many Internet Service Providers (ISP) as well as Enterprises to authenticate dial in users. Today, many businesses use the RADIUS server for authenticating users connecting into a network. For example, if a user connects PC into the network, whether the PC should be allowed access or not provides the same issues as to whether or not a dial in user should be allowed access into the network or not. A user has to provide a user name and password for authenticated access. A RADIUS server is well suited for controlling access into a network by managing the users who can access the network on a RADIUS server. Interacting with the server and taking corrective action(s) is not possible on all switches. This capability is provided on the MultiLink family of switches.

RADIUS servers and its uses are also described by one or more RFCs.

7.1.2 802.1x Protocol

There are three major components of 802.1x: - Supplicant, Authenticator and Authentication Server (RADIUS Server). In the figure below, the PC acts as the supplicant. The supplicant is an entity being authenticated and desiring access to the services. The switch is the authenticator. The authenticator enforces authentication before allowing

access to services that are accessible via that port. The authenticator is responsible for communication with the supplicant and for submitting the information received from the supplicant to a suitable authentication server. This allows the verification of user credentials to determine the consequent port authorization state. It is important to note that the authenticator's functionality is independent of the actual authentication method. It effectively acts as a pass-through for the authentication exchange.

FIGURE 7–1: 802.1x network components

The RADIUS server is the authentication server. The authentication server provides a standard way of providing Authentication, Authorization, and Accounting services to a network. Extensible Authentication Protocol (EAP) is an authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as PPP or IEEE 802, without requiring IP. EAP over LAN (EAPOL) encapsulates EAP packets onto 802 frames with a few extensions to handle 802 characteristics. EAP over RADIUS encapsulates EAP packets onto RADIUS packets for relaying to RADIUS authentication servers.

The details of the 802.1x authentication are as follows.

1. The supplicant (host) is initially blocked from accessing the network. The supplicant wanting to access these services starts with an EAPOL-Start frame.
2. The authenticator (MultiLink switch), upon receiving an EAPOL-start frame, sends a response with an EAP-Request/Identity frame back to the supplicant. This will inform the supplicant to provide its identity.
3. The supplicant then sends back its own identification using an EAP-Response/ Identity frame to the authenticator (MultiLink switch.) The authenticator then relays this to the authentication server by encapsulating the EAP frame on a RADIUS-Access-Request packet.
4. The RADIUS server will then send the authenticator a RADIUS-Access-Challenge packet.
5. The authenticator (MultiLink switch) will relay this challenge to the supplicant using an EAP-Request frame. This will request the supplicant to pass its credentials for authentication.
6. The supplicant will send its credentials using an EAP-Response packet.
7. The authenticator will relay using a RADIUS-Access-Request packet.
8. If the supplicant's credentials are valid, RADIUS-Access-Accept packet is sent to the authenticator.
9. The authenticator will then relay this on as an EAP-Success and provides access to the network.

10. If the supplicant does not have the necessary credentials, a RADIUS-Access-Deny packet is relayed to the supplicant as an EAP-Failure frame. The access to the network continues to be blocked.

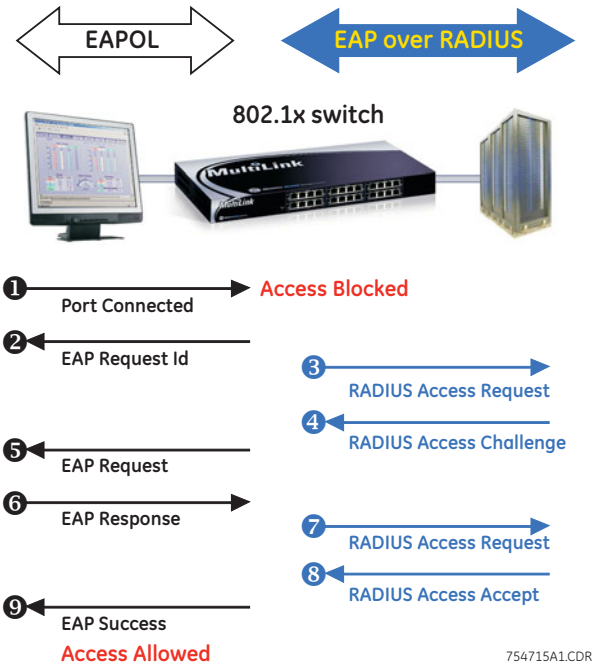


FIGURE 7–2: 802.1x authentication details

The ML2400 software implements the 802.1x authenticator. It fully conforms to the standards as described in IEEE 802.1x, implementing all the state machines needed for port-based authentication. The ML2400 software authenticator supports both EAPOL and EAP over RADIUS to communicate to a standard 802.1x supplicant and RADIUS authentication server.

The ML2400 software authenticator has the following characteristics:

- Allows control on ports using STP-based hardware functions. EAPOL frames are Spanning Tree Protocol (STP) link Bridge PDUs (BPDU) with its own bridge multicast address.
- Relays MD5 challenge (although not limited to) authentication protocol to RADIUS server
- Limits the authentication of a single host per port
- The MultiLink switch provides the IEEE 802.1x MIB for SNMP management

7.2 Configuring 802.1x through the Command Line Interface

7.2.1 Commands

On enabling 802.1x ports, make sure the port which connects to the RADIUS servers needs to be manually authenticated. To authenticate the port, use the `setport` command. The CLI commands to configure and perform authentication with a RADIUS server are described below.

The `auth` command enters the configuration mode to configure the 802.1x parameters.

auth

The `show auth` command displays the 802.1x configuration or port status.

show auth *<config|ports>*

The `authserver` command define the RADIUS server. Use the UDP socket number if the RADIUS authentication is on a port other than 1812.

authserver *[ip=<ip-addr>] [udp=<num>] [secret=<string>]*

The `auth enable` and `auth disable` commands enable or disable the 802.1x authenticator function on the MultiLink switch.

auth *<enable|disable>*

The `setport` command configures the port characteristics for an 802.1x network.

setport *port=<num|list|range> [status=<enable|disable>]*
[control=<auto|forceauth|forceunauth>] [initialize=<assert|deassert>]

The `backend port` command configure the parameters for EAP over RADIUS.

backend *port=<num|list|range>*
[supptimeout=<1-240>]
[servertimeout=<1-240] [maxreq=<1-10>]

The `port` argument is mandatory and represents the port(s) to be configured. The `supptimeout` argument is optional and represents the timeout in seconds the authenticator waits for the supplicant to respond back. The default value is 30 seconds and values can range from 1 to 240 seconds. The `servertimeout` argument is optional and represents the timeout in seconds the authenticator waits for the back-end RADIUS server to respond. The default value is 30 seconds and can range from 1 to 240 seconds. The `maxreq` argument is optional and represents the maximum number of times the authenticator will retransmit an EAP request packet to the Supplicant before it times out the authentication session. Its default value is 2 and can be set to any integer value from 1 to 10.

The `portaccess` command sets port access parameters for authenticating PCs or supplicants.

portaccess *port=<num|list|range>*
[quiet=<0-65535>] [maxreauth=<0-10>] [transmit=<1-65535>]

The `port` argument is mandatory and identifies the ports to be configured. The `quiet` argument is optional and represents the quiet period – the amount of time, in seconds, the supplicant is held after an authentication failure before the authenticator retries the supplicant for connection. The default value is 60 seconds and values can range from 0 to 65535 seconds. The `maxreauth` argument is optional and represents the number of re-authentication attempts permitted before the port is unauthorized. The default value is 2

and integer values can range from 0 to 10. The **transmit** argument is optional and represents the transmit period. This is the time in seconds the authenticator waits to transmit another request for identification from the supplicant. The default value is 30 and values range from 1 to 65535 seconds

The **reauth** command determines how the authenticator (MultiLink switch) performs the re-authentication with the supplicant or PC.

reauth *port=<num|list|range> [status=<enable|disable>] [period=<10-86400>]*

The port argument is mandatory and sets the ports to be configured. The status argument is optional and enables/disables re-authentication. The period argument is optional and represents the re-authentication period. This is the time in seconds the authenticator waits before a re-authentication process will be performed again to the supplicant. The default value is 3600 seconds (1 hour), and values range from 10 to 86400 seconds.

The **show-stats** command displays 802.1x related statistics.

show-stats *port=<num>*

The **trigger-reauth** command manually initiates a re-authentication of supplicant.

trigger-reauth *port=<num|list|range>*

7.2.2 Example

Example 7-1 demonstrates how to secure the network using port access. Ensure there is no 802.1x or RADIUS server defined. Only one RADIUS server can be defined for the entire network.

Example 7-1: Setting port control parameters

```
802.1X Authenticator Configuration
==================================
Status: Disabled
RADIUS Authentication Server
==================================
  IP Address:        0.0.0.0
  UDP Port:          1812
  Shared Secret:
ML2400# auth
ML2400(auth)## setport port=2 status=enable control=forceauth initialize=assert
  Successfully set port control parameter(s)
ML2400(auth)## auth disable
  802.1X Authenticator is disabled.
ML2400(auth)## authserver ip=3.204.240.1 secret=secret
  Successfully set RADIUS Authentication Server parameter(s)
ML2400(auth)## auth enable
  802.1X Authenticator is enabled.
ML2400(auth)## show auth ports
Port  Status    Control     Initialize   Current State
=====================================================
1     Enabled   Auto        Deasserted   Authorized
2     Enabled   ForcedAuth  Asserted     Unauthorized
3     Enabled   Auto        Deasserted   Authorized
4     Enabled   Auto        Deasserted   Unauthorized
5     Enabled   Auto        Deasserted   Unauthorized
6     Enabled   Auto        Deasserted   Unauthorized
7     Enabled   Auto        Deasserted   Unauthorized
8     Enabled   Auto        Deasserted   Unauthorized
9     Enabled   Auto        Deasserted   Unauthorized
10    Enabled   Auto        Deasserted   Unauthorized
11    Enabled   Auto        Deasserted   Unauthorized
12    Enabled   Auto        Deasserted   Unauthorized
13    Enabled   Auto        Deasserted   Unauthorized
14    Enabled   Auto        Deasserted   Unauthorized
15    Enabled   Auto        Deasserted   Unauthorized
16    Enabled   Auto        Deasserted   Unauthorized
-- Port not available
ML2400(auth)## show auth config
802.1X Authenticator Configuration
==================================
Status: Enabled
RADIUS Authentication Server
==================================
  IP Address:         3.204.240.1
  UDP Port:           1812
  Shared Secret:      secret
```

The RADIUS server is on port 2. This port is authenticated manually. If the RADIUS server is several hops away, it may be necessary to authenticate the interconnection ports. Make sure the `setport port=2 status=enable control=forceauth initialize=assert` command is executed before the `auth enable` command.

The `auth disable` command is not necessary. However, it is shown for completeness in case a RADIUS server was defined with a previously set authentication scheme.

The RADIUS server is connected on port #2

(continued on following page)

Setting port control parameters (continued)

```
ML2400(auth)## backend port=2 supptimeout=45 servertimeout=60 maxreq=5

  Successfully set backend server authentication
  parameter(s)
```

This command sets timeout characteristics and the number of requests before access is denied.

```
ML2400(auth)## show-port backend

Port   Supp Timeout   Server Timeout   Max Request
          (sec.)          (sec.)
================================================
1           30              30            2
2           45              60            5
3           30              30            2
4           30              30            2
5           30              30            2
6           30              30            2
7           30              30            2
8           30              30            2
9           30              30            2
10          30              30            2
11          30              30            2
12          30              30            2
13          30              30            2
14          30              30            2
15          30              30            2
16          30              30            2
```

The authenticator waits for the supplicant to respond back for 45 seconds; the authenticator waits for 60 seconds for the back-end RADIUS server to respond back and the authenticator will retransmit an EAP request packet 5 times to the Supplicant before it times out the authentication session.

```
ML2400(auth)## portaccess port=2 quiet=120 maxreauth=7 transmit=120

  Successfully set port access parameter(s)

ML2400(auth)## show-port access

Port   Quiet Period   Max Reauth   Tx Period
          (sec.)       (sec.)
========================================
1           60            2            30
2           120           7            120
3           60            2            30
4           60            2            30
5           60            2            30
6           60            2            30
7           60            2            30
8           60            2            30
9           60            2            30
10          60            2            30
11          60            2            30
12          60            2            30
13          60            2            30
14          60            2            30
15          60            2            30
16          60            2            30
```

The time the supplicant is held after an authentication failure before the authenticator retries the supplicant for connection is changed to 120 seconds, the number of re-authentication attempts permitted before the port becomes Unauthorized is set to 7, and the time the authenticator waits to transmit another request for identification from the supplicant is changed to 120 seconds. These values can be changed on all ports depending on devices being authenticated.

(continued on following page)

Setting port control parameters (continued)

```
ML2400(auth)## reauth port=1 status=enable period=300

  Successfully set re-authentication parameter(s)
ML2400(auth)## show-port reauth

Port  Reauth Status  Reauth Period (sec.)
=======================================
1          Enabled         300
2          Enabled         3600
3          Enabled         3600
4          Enabled         3600
5          Enabled         3600
6          Enabled         3600
7          Enabled         3600
8          Enabled         3600
9          Enabled         3600
10         Enabled         3600
11         Enabled         3600
12         Enabled         3600
13         Enabled         3600
14         Enabled         3600
15         Enabled         3600
16         Enabled         3600
ML2400(auth)## show-stats port=3

  Port 3 Authentication Counters

  authEntersConnecting                  : 3
  authEapLogoffsWhileConnecting         : 0
  authEntersAuthenticating              : 3
  authAuthSuccessesWhileAuthenticating  : 2
  authAuthTimeoutsWhileAuthenticating   : 0
  authAuthFailWhileAuthenticating       : 0
  authAuthReauthsWhileAuthenticating    : 0
  authAuthEapStartsWhileAuthenticating  : 1
  authAuthEapLogoffWhileAuthenticating  : 0
  authAuthReauthsWhileAuthenticated     : 0
  authAuthEapStartsWhileAuthenticated   : 0
  authAuthEapLogoffWhileAuthenticated   : 0
  backendResponses                      : 5
  backendAccessChallenges               : 2
  backendOtherRequestsToSupplicant      : 0
  backendNonNakResponsesFromSupplicant  : 2
  backendAuthSuccesses                  : 2
  backendAuthFails                      : 0
ML2400(auth)## trigger-reauth port=3

  Successfully triggered re-authentication
ML2400(auth)##
```

This command forces the authentication period on port #1 every 5 minutes; all other ports are force authenticated every hour as indicated by the `show-port reauth` command below.

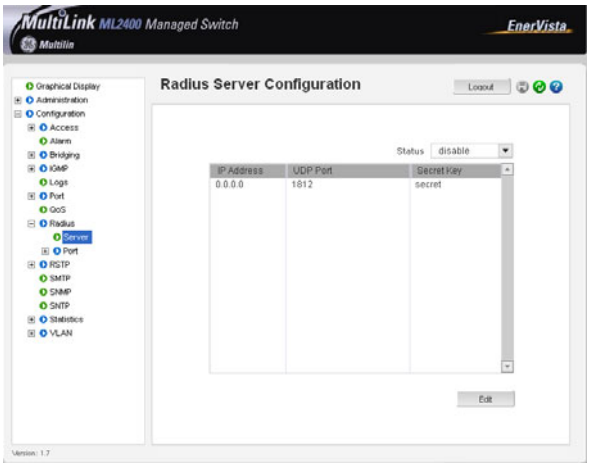
7.3 Configuring 802.1x with EnerVista Secure Web Management Software

7.3.1 Commands

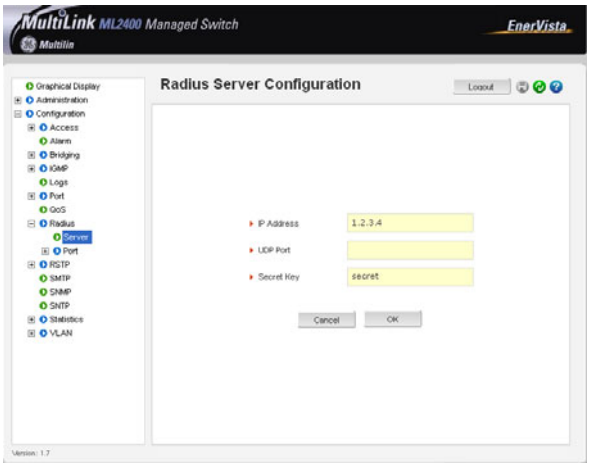
To access the 802.1x configuration window, select the **Configuration > Radius > Server** menu item.

First, select the server. *Do not enable RADIUS capabilities until you have ensured that the ports are configured properly*. After the ports are configured, enable RADIUS. Also ensure that the port connected to the RADIUS server, or the network where the RADIUS server is connected to, is not an authenticated port.

The following window shows the configuration of a RADIUS Server. Initially, the RADIUS Services are disabled and the server IP address is set to 0.0.0.0. Edit the server IP and secret to add a RADIUS server.



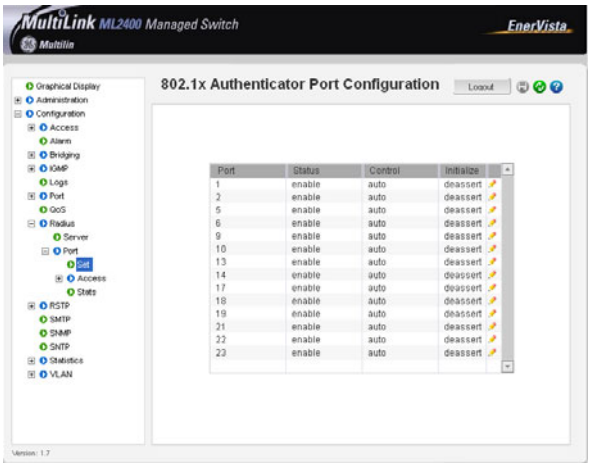
The following figure illustrates the editing of information for the RADIUS server. Note the UDP port number can be left blank and the default port 1812 is used.



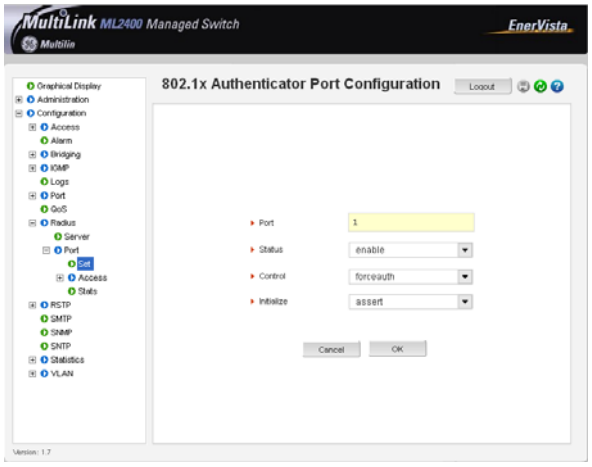
After configuring the server information, specific port information is configured.

▷ Select the **Configuration > Radius > Port > Set** menu item to configure the RADIUS characteristics of each port.

▷ To edit the port settings, click on the edit icon ( ).

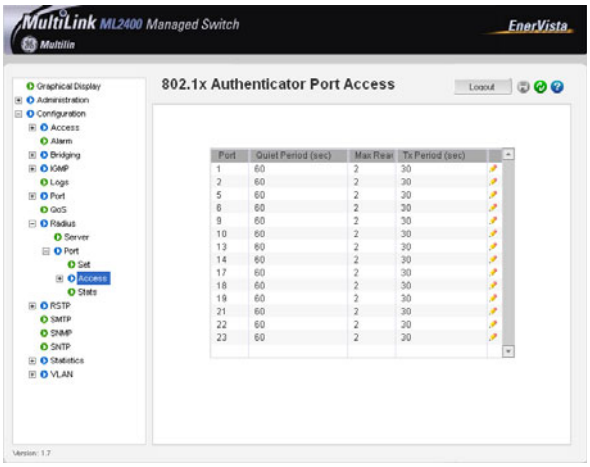


Ensure that the port which has the RADIUS server is force authorized and asserted. For other ports (user ports), it is best to leave the **Control** on auto and **Initialize** on de-asserted.



To change the port access characteristics when authenticating with a RADIUS server,

▷ Select the **Configuration > Radius > Port > Access** menu item.

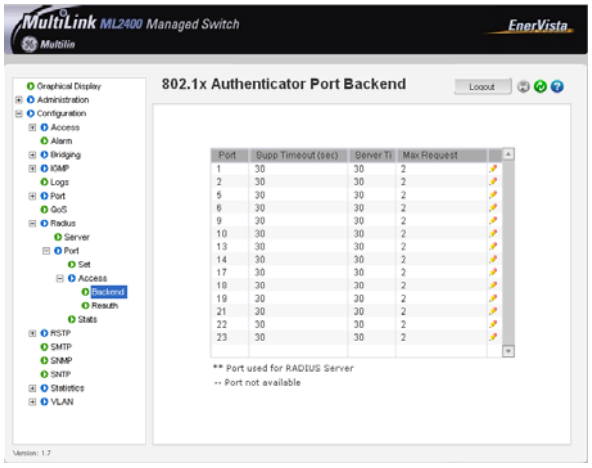


The **Quiet Period** column represents the time, in seconds, the supplicant is held after an authentication failure before the authenticator retries the supplicant for connection. The value ranges from 0 to 65535 seconds, with a default of 60.

The **Max Reauth** column shows the permitted reauthentication attempts before the port becomes unauthorized. Values are integers ranging from 0 to 10, with a default of 2.

The **Tx Period** column represents the transmit period. This is the time (in seconds) the authenticator waits to transmit another request for identification from the supplicant. The values range from 1 to 65535 seconds, with a default of 30.

The backend or communication characteristics between the ML2400 and the RADIUS Server are defined through the **Configuration > Radius > Port > Access > Backend** menu item.

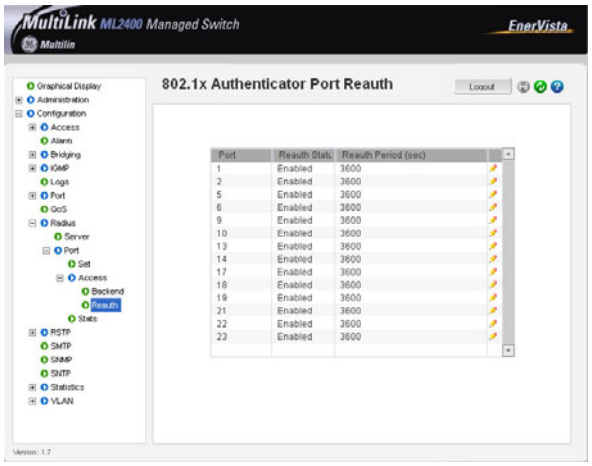


The **Supp Timeout** column represents the timeout the authenticator waits for the supplicant to respond. The values range from 1 to 240 seconds, with a default of 30.

The **Server Timeout** column represents the timeout the authenticator waits for the backend RADIUS server to respond. The values range from 1 to 240 seconds, with a default of 30.

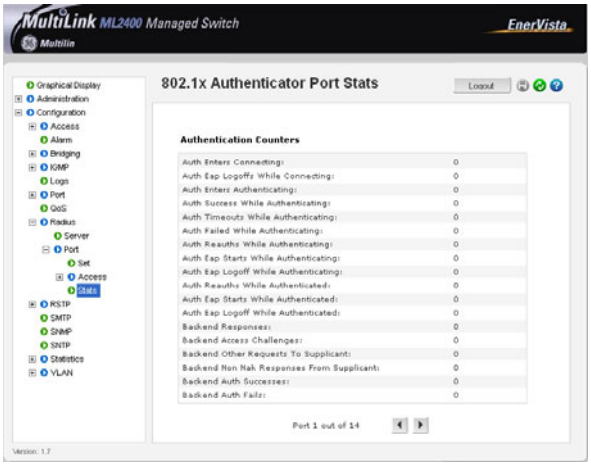
The **Max Request** column represents the maximum times the authenticator retransmits an EAP request packet to the supplicant before it times out. Values are integers ranging from 1 to 10, with a default of 2.

The port authentication characteristics define how the authenticator (ML2400 switch) does the re-authentication with the supplicant or PC. These are defined through the **Configuration > Radius > Port > Access > Reauth** menu item.



The **Reauth Period** represents the time the authenticator waits before a re-authentication process will be done again to the supplicant. Values range from 10 to 86400 seconds, with a default of 3600 (1 hour).

The **Configuration > Radius > Port > Stats** menu item illustrates the radius statistics for each port.


MultiLink ML2400 Managed Switch
EnerVista
802.1x Authenticator Port Stats
Logout
Authentication Counters
Auth Enters Connecting: 0
Auth Eap Logoffs While Connecting: 0
Auth Enters Authenticating: 0
Auth Success While Authenticating: 0
Auth Timeouts While Authenticating: 0
Auth Failed While Authenticating: 0
Auth Reauths While Authenticating: 0
Auth Eap Starts While Authenticating: 0
Auth Eap Logoff While Authenticating: 0
Auth Reauths While Authenticated: 0
Auth Eap Starts While Authenticated: 0
Auth Eap Logoff While Authenticated: 0
Backend Responses: 0
Backend Access Challenges: 0
Backend Other Requests To Supplicant: 0
Backend Non Nak Responses From Supplicant: 0
Backend Auth Successes: 0
Backend Auth Fails: 0
Port 1 out of 14

After all the port characteristics are enabled,

▷ **Do not forget** to save the configuration using the save ( ) icon and enabling RADIUS from the **Configuration > Radius > Server** menu.

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 8: Access using TACACS+

8.1 Introduction to TACACS+

8.1.1 Overview

The TACACS+ protocol (short for Terminal Access Controller Access Control System) provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon (server) or simply TACACSD. This server was normally a program running on a host. The host would determine whether to accept or deny the request and sent a response back.

The TACACS+ protocol is the latest generation of TACACS. TACACS is a simple UDP based access control protocol originally developed by BBN for the MILNET (Military Network). XTACACS is now replaced by TACACS+. TACACS+ is a TCP based access control protocol. TCP offers a reliable connection-oriented transport, while UDP offers best-effort delivery.

TACACS+ improves on TACACS and XTACACS by separating the functions of authentication, authorization and accounting and by encrypting all traffic between the Network Access Server (NAS) and the TACACS+ clients or services or daemon. It allows for arbitrary length and content authentication exchanges, which allows any authentication mechanism to be utilized with TACACS+ clients. The protocol allows the TACACS+ client to request very fine-grained access control by responding to each component of a request.

The MultiLink switch implements a TACACS+ client.

1. TACACS+ servers and daemons use TCP port 49 for listening to client requests. Clients connect to this port to send authentication and authorization packets.
2. There can be more than one TACACS+ server on the network. The MultiLink Switch Software supports a maximum of five TACACS+ servers.

8.1.2 TACACS+ Flow

TACACS works in conjunction with the local user list on the ML2400 software (operating system). Please refer to *User Management* on page 1–14 for adding users on the MultiLink Switch Software. The process of authentication as well as authorization is shown in the flow chart below.

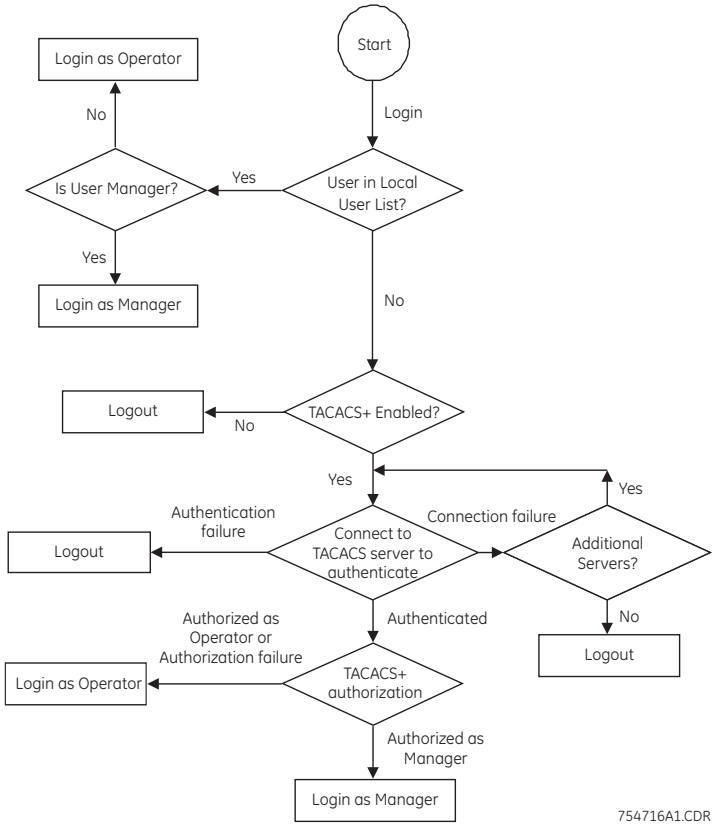


FIGURE 8–1: TACACS Authorization Flowchart

The above flow diagram shows the tight integration of TACACS+ authentication with the local user-based authentication. There are two stages a user goes through in TACACS+. The first stage is authentication where the user is verified against the network user database. The second stage is authorization, where it is determined whether the user has operator access or manager privileges.

8.1.3 TACACS+ Packet

Packet encryption is a supported and is a configurable option for the ML2400 software. When encrypted, all authentication and authorization TACACS+ packets are encrypted and are not readable by protocol capture and sniffing devices such as EtherReal or others. Packet data is hashed and shared using MD5 and secret string defined between the MultiLink switches and the TACACS+ server.

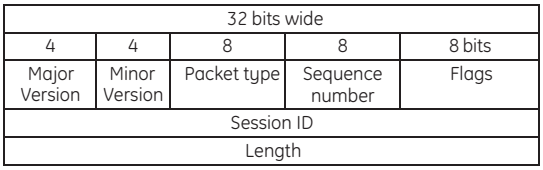


FIGURE 8–2: TACACS packet format

The portions of the TACACS packet are defined as follows:

- **Major Version**: The major TACACS+ version number.
- **Minor version**: The minor TACACS+ version number. This is intended to allow revisions to the TACACS+ protocol while maintaining backwards compatibility.
- **Packet type**: Possible values are:
- TAC_PLUS_AUTHEN:= 0x01 (authentication)
  TAC_PLUS_AUTHOR:= 0x02 (authorization)
  TAC_PLUS_ACCT:= 0x03 (accounting)
- **Sequence number**: The sequence number of the current packet for the current session.
- **Flags**: This field contains various flags in the form of bitmaps. The flag values signify whether the packet is encrypted.
- **Session ID**: The ID for this TACACS+ session.
- **Length**: The total length of the TACACS+ packet body (not including the header).

8.2 Configuring TACACS+ through the Command Line Interface

8.2.1 Commands

There are several commands to configure TACACS+.

The `show tacplus` command displays the status of TACACS or servers configured as TACACS+ servers:

show tacplus *<status|servers>*

The `tacplus enable` and `tacplus disable` commands enable or disable TACACS authentication:

tacplus *<enable|disable>*

The `tacserver` command creates a list of up to five TACACS+ servers:

tacserver *<add|delete> id=<num>*
[ip=<ip-addr>] [port=<tcp-port>] [encrypt=<enable|disable>] [key=<string>]

The <**`add|delete`**> argument is mandatory and specifies whether to add or delete a TACACS+ server. The **`id`** argument is mandatory and sets the order to poll the TACACS+ servers for authentication. The **`ip`** argument is mandatory for adding and defines the IP address of the TACACS+ server. The **`port`** argument is mandatory for deleting and defines the TCP port number on which the server is listening. The **`encrypt`** argument enables or disables packet encryption and is mandatory for deleting. The **`key`** argument requires the secret shared key string must be supplied when encryption is enabled.

8.2.2 Example

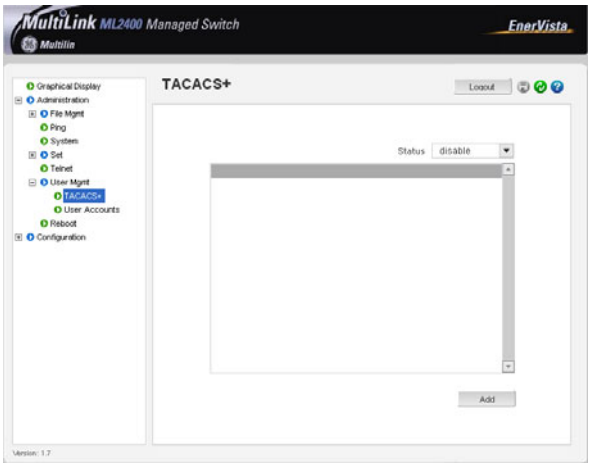
Example 8-1 illustrates how to configure TACACS+.

Example 8-1: Configuring TACACS+:

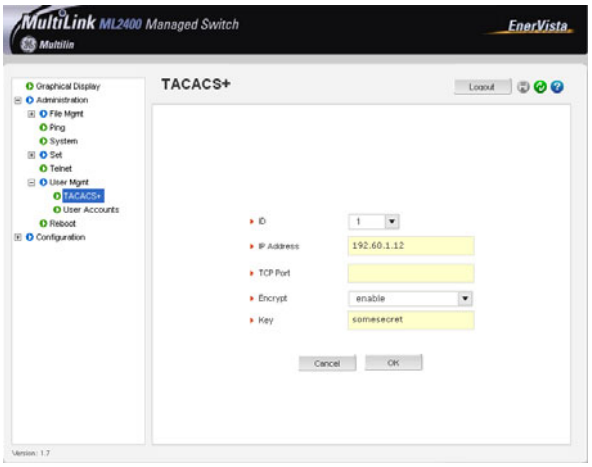
```
ML2400# show tacplus servers
 ID  TACACS+ Server  Port  Encrypt   Key
 ========================================
 1   10.21.1.170     49    Enabled   secret
 2   --              --    --        --
 3   --              --    --        --
 4   --              --    --        --
 5   --              --    --        --
ML2400# user
ML2400(user)## show tacplus status
  TACACS+ Status: Disabled
ML2400(user)## tacplus enable
  TACACS+ Tunneling is enabled.
ML2400(user)## tacserver add id=2 ip=10.21.1.123 encrypt=enable k
  TACACS+ server is added.
ML2400(user)## show tacplus servers
 ID  TACACS+ Server  Port  Encrypt   Key
 ========================================
 1   10.21.1.170     49    Enabled   secret
 2   10.21.1.123     49    Enabled   some
 3   --              --    --        --
 4   --              --    --        --
 5   --              --    --        --
ML2400(user)## tacserver delete id=2
  TACACS+ server is deleted.
ML2400(user)## show tacplus servers
 ID  TACACS+ Server  Port  Encrypt   Key
 ========================================
 1   10.21.1.170     49    Enabled   secret
 2   --              --    --        --
 3   --              --    --        --
 4   --              --    --        --
 5   --              --    --        --
ML2400(user)## tacplus disable
  TACACS+ is disabled.
ML2400(user)##
```

8.3 Configuring TACACS+ with EnerVista Secure Web Management Software

▷ To access the TACACS servers, select the **Administration > User Mgmt > TACACS+** menu item.
By default, no TACACS servers are defined.



▷ To add a server, click on the Add button as shown below.

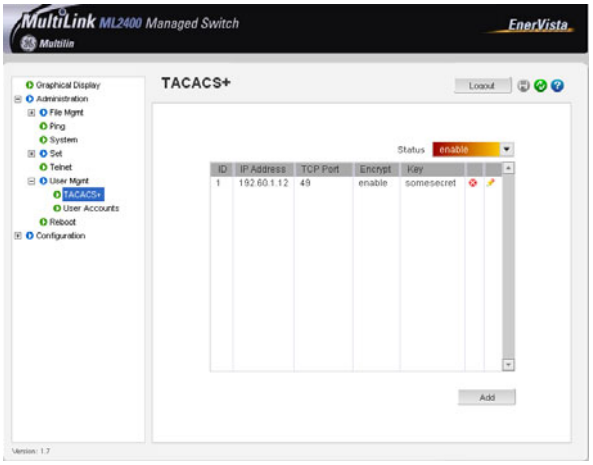


Note that the TCP port field can be left blank – port 49 is used as a default port. Up to five TACACS+ servers can be defined.

After the configuration is completed,

▷ Save the settings.

▷ Enable the TACACS+ services by using the **Status** drop down menu.


MultiLink ML2400 Managed Switch
Multilin
EnerVista
Graphical Display
Administration
File Mgmt
Ping
System
Set
Telnet
User Mgmt
TACACS+
User Accounts
Reboot
Configuration
TACACS+
Logout
Status
enable
ID
IP Address
TCP Port
Encrypt
Key
1
192.60.1.12
49
enable
somesecret
Add

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 9: Port Mirroring and Setup

9.1 Port Mirroring

9.1.1 Description

This section explains how individual characteristics of a port on a GE MultiLink switch is configured. For monitoring a specific port, the traffic on a port can be mirrored on another port and viewed by protocol analyzers. Other setup includes automatically setting up broadcast storm prevention thresholds.

An Ethernet switch sends traffic from one port to another port. Unlike a switch, a hub or a shared network device, the traffic is “broadcast” on each and every port. Capturing traffic for protocol analysis or intrusion analysis can be impossible on a switch unless all the traffic from a specific port is “reflected” on another port, typically a monitoring port. The MultiLink family of switches can be instructed to repeat the traffic from one port onto another port. This process - when traffic from one port is reflecting to another port - is called port mirroring. The monitoring port is also called a “sniffing” port. Port monitoring becomes critical for trouble shooting as well as for intrusion detection.

9.2 Port Mirroring using the Command Line Interface

9.2.1 Commands

Monitoring a specific port can be done by port mirroring. Mirroring traffic from one port to another port allows analysis of the traffic on that port.

The `show port-mirror` command displays the status of port mirroring:

show port-mirror

The `port-mirror` command enters the port mirror configuration mode.

port-mirror

The `setport monitor` command configures a port mirror.

setport *monitor=<monitor port number> sniffer=<sniffer port number>*

The `prtmr` command enables and disables port mirroring.

prtmr *<enable|disable>*

The sequence below illustrates how port 11 is mirrored on port 13. Any traffic on port 11 is also sent on port 13.

ML2400# `show port-mirror`

```
Sniffer Port: 0
Monitor Port: 0
Mirroring State: disabled
```

ML2400# `port-mirror`

ML2400(port-mirror)## `setport monitor=11 sniffer=13`

```
Port 11 set as Monitor Port
Port 13 set as Sniffer Port
```

ML2400(port-mirror)## `prtmr enable`

```
Port Mirroring Enabled
```

ML2400(port-mirror)## `exit`

ML2400# `show port-mirror`

```
Sniffer Port: 13
Monitor Port: 11
Mirroring State: enabled
```

ML2400#

Once port monitoring is completed, GE strongly recommends that the port mirroring be disabled using the `prtmr disable` command for security reasons.

1. Only one port can be set to port mirror at a time.
2. Both the ports (monitored port and mirrored port) have to belong to the same VLAN
3. The mirrored port shows bout incoming as well as outgoing traffic

9.3 Port Setup

9.3.1 Commands

Each port on the GE MultiLink family of switches can be setup specific port characteristics. The commands for setting the port characteristics are shown below.

The `device` command enters the device configuration mode:

device

The `setport` command configures the port characteristics:

setport *port=<port#|list|range> [name=<name>] [speed=<10|100>] [duplex=<half|full>] [auto=<enable|disable>] [flow=<enable|disable>] [bp=<enable|disable>] [status=<enable|disable>] [lla=<enable|disable>]*

The arguments for the `setport` command are defined as follows:

- The `device` argument sets up the MultiLink switch in the device configuration mode.
- The `name` argument assigns a specific name to the port. This name is a designated name for the port and can be a server name, user name or any other name.
- The `speed` argument sets the speed to be 10 or 100 Mbps. This works only with 10/100 ports; the value is ignored and no error shown for 10 Mbps ports.
- The `flow` argument sets up flow control on the port.
- The `bp` argument enables back pressure signaling for traffic congestion management.
- The `status` argument enabled/disables port operation

The show port command displays information about a specific port number.

show port*[=<port number>]*

In Example 9-1, ports 11 and 12 are given specific names. Ports 9 and 13 are active, as shown by the link status. Port 13 is set to 100 Mbps, and all other ports are set to 10 Mbps. All ports are set to auto sensing (speed).

The port **speed** and **duplex** (data transfer operation) settings are summarized below.

The **speed** setting defaults to auto and senses speed and negotiates with the port at the other end of the link for data transfer operation (half-duplex or full-duplex). The "auto" speed detection uses the IEEE 802.3u auto negotiation standard for 100Base-T networks. If the other device does not comply with the 802.3u standard, then the port configuration on the switch must be manually set to match the port configuration on the other device.

Possible port setting combinations for copper ports are:

- 10HDx: 10 Mbps, half-duplex
- 10FDx: 10 Mbps, full-duplex
- 100HDx: 100 Mbps, half-duplex
- 100FDx: 100 Mbps, full-duplex

Possible port settings for 100FX (fiber) ports are:

- 100FDx (default): 100 Mbps, full-duplex
- 100HDx: 100 Mbps, half-duplex

Possible port settings for 10FL (fiber) ports are:

- 10HDx (default): 10 Mbps, half-duplex
- 10FDx: 10 Mbps, full-duplex

Gigabit fiber-optic ports (Gigabit-SX and Gigabit-LX):

- 1000FDx (default): 1000 Mbps, full-duplex only
- Auto: The port operates at 1000FDx and auto-negotiates flow control with the connected device.

Example 9-1: Port setup

```
ML2400# device
ML2400(device)## setport port=11 name=JohnDoe
ML2400(device)## setport port=12 name=JaneDoe
ML2400(device)## show port
Keys: E  = Enable              D  = Disable
      H  = Half Duplex         F  = Full Duplex
      M  = Multiple VLAN's     NA = Not Applicable
      LI = Listening           LE = Learning
      F  = Forwarding          B  = Blocking

Port  Name     Control  Dplx  Media  Link  Speed  Part  Auto  VlanID  GVRP  STP
-------------------------------------------------------------------------------
 9    B1       E        H     10Tx   UP    10     No    E     1       -     -
10    B2       E        H     10Tx   DOWN  10     No    E     1       -     -
11    JohnDoe  E        H     10Tx   DOWN  10     No    E     1       -     -
12    JaneDoe  E        H     10Tx   DOWN  10     No    E     1       -     -
13    B5       E        F     100Tx  UP    100    No    E     1       -     -
14    B6       E        H     10Tx   DOWN  10     No    E     1       -     -
15    B7       E        H     10Tx   DOWN  10     No    E     1       -     -
16    B8       E        H     10Tx   DOWN  10     No    E     1       -     -
ML2400(device)## exit
ML2400#
```

NOTE

To change the port speed on a transceiver port, it is required to reboot the switch.

9.3.2 Flow Control

The `flow` setting is disabled by default. In this case, the port will not generate flow control packets and drops received flow control packets. If the `flow` setting is enabled, the port uses 802.3x Link Layer Flow Control, generates flow control packets, and processes received flow control packets.

NOTE

With the port speed set to auto (the default) and flow control set to enabled; the switch negotiates flow control on the indicated port. If the port speed is not set to auto, or if flow control is disabled on the port, then flow control is not used.

Use the `flowcontrol` command to set flow control:

flowcontrol *xonlimit=<value> xofflimit=<value>*

where `xonlimit` can be from 3 to 127 (default value is 4) and `xofflimit` ranges from 3 to 127 (default value is 6).

9.3.3 Back Pressure

The `backpressure` command disables/enables back pressure based flow control mechanisms. The default state is disabled. When enabled, the port uses 802.3 Layer 2 back off algorithms. Back pressure based congestion control is possible only on half-duplex, 10-Mbps Ethernet ports. Other technologies are not supported on the MultiLink family of switches.

backpressure *rxthreshold=<value>*

where the `rxthreshold` value can be from 4 to 30 (default is 28).

Back pressure and flow control are used in networks where all devices and switches can participate in the flow control and back pressure recognition. In most networks, these techniques are not used as not all devices can participate in the flow control methods and notifications. Alternately, QoS and other techniques are widely used today.

In the example below, the MultiLink family of switches are setup with flow control and back pressure.

Example 9-2: Back pressure and flow control

```
ML2400# device
ML2400(device)## show flowcontrol
  XOnLimit  : 4
  XOffLimit : 6
ML2400(device)## flowcontrol xonlimit=10 xofflimit=15
  XOn Limit set successfully
  XOff Limit set successfully
ML2400(device)## show flowcontrol
  XOnLimit  : 10
  XOffLimit : 15
ML2400(device)## show backpressure
  Rx Buffer Threshold : 28
```

(continued on next page)

Back pressure and flow control (continued)

```
ML2400(device)## backpressure rxthreshold=30

  Rx Buffer Threshold set successfully
ML2400(device)## show backpressure

  Rx Buffer Threshold : 30
ML2400(device)## show port

Keys:  E  = Enable            D  = Disable
       H  = Half Duplex       F  = Full Duplex
       M  = Multiple VLAN's   NA = Not Applicable
       LI = Listening         LE = Learning
       F  = Forwarding        B  = Blocking

Port  Name     Control  Dplx  Media  Link  Speed  Part  Auto  VlanID  GVRP  STP
-------------------------------------------------------------------------------
 9    B1       E        H     10Tx   UP    10     No    E     1       -     -
10    B2       E        H     10Tx   DOWN  10     No    E     1       -     -
11    JohnDoe  E        H     10Tx   DOWN  10     No    E     1       -     -
12    JaneDoe  E        H     10Tx   DOWN  10     No    E     1       -     -
13    B5       E        F     100Tx  UP    100    No    E     1       -     -
14    B6       E        H     10Tx   DOWN  10     No    E     1       -     -
15    B7       E        H     10Tx   DOWN  10     No    E     1       -     -
16    B8       E        H     10Tx   DOWN  10     No    E     1       -     -
ML2400(device)## show port=11

Configuration details of port 11
-------------------------------------------------
Port Name                       : JohnDoe
Port Link State                 : DOWN
Port Type                       : TP Port
Port Admin State                : Enable
Port VLAN ID                    : 1
Port Speed                      : 10Mbps
Port Duplex Mode                : half-duplex
Port Auto-negotiation State     : Enable
Port STP State                  : NO STP
Port GVRP State                 : No GVRP
Port Priority Type              : None
Port Security                   : Enable
Port Flow Control               : Disable
Port Back Pressure              : Disable
Port Link Loss Alert            : Enabled
ML2400(device)## setport port=11 flow=enable bp=enable
```

(continued on next page)

Back pressure and flow control (continued)

```
ML2400(device)## show port

Keys:  E  = Enable            D  = Disable
       H  = Half Duplex       F  = Full Duplex
       M  = Multiple VLAN's   NA = Not Applicable
       LI = Listening         LE = Learning
       F  = Forwarding        B  = Blocking

Port  Name      Control  Dplx  Media  Link  Speed  Part  Auto  VlanID  GVRP  STP
-------------------------------------------------------------------------------
 9    B1        E        H     10Tx   UP    10     No    E     1       -     -
10    B2        E        H     10Tx   DOWN  10     No    E     1       -     -
11    JohnDoe   E        H     10Tx   DOWN  10     No    E     1       -     -
12    JaneDoe   E        H     10Tx   DOWN  10     No    E     1       -     -
13    B5        E        F     100Tx  UP    100    No    E     1       -     -
14    B6        E        H     10Tx   DOWN  10     No    E     1       -     -
15    B7        E        H     10Tx   DOWN  10     No    E     1       -     -
16    B8        E        H     10Tx   DOWN  10     No    E     1       -     -

ML2400(device)## show port=11

Configuration details of port 11
-------------------------------------------------
Port Name                        : JohnDoe
Port Link State                  : DOWN
Port Type                        : TP Port
Port Admin State                 : Enable
Port VLAN ID                     : 1
Port Speed                       : 10Mbps
Port Duplex Mode                 : half-duplex
Port Auto-negotiation State      : Enable
Port STP State                   : NO STP
Port GVRP State                  : No GVRP
Port Priority Type               : None
Port Security                    : Enable
Port Flow Control                : Enable
Port Back Pressure               : Enable
Port Link Loss Alert             : Enabled
```

Note that the flow control and back pressure is shown as enabled for the specific port. The global `show port` command does not provide this detail. The back pressure and flow control parameters are global – i.e., the same for all ports.

9.3.4 Broadcast Storms

One of the best features of the MultiLink family of switches is its ability to keep broadcast storms from spreading throughout a network. Network storms (or broadcast storms) are characterized by an excessive number of broadcast packets being sent over the network. These storms can occur if network equipment is configured incorrectly. Storms can reduce network performance and cause bridges, routers, workstations, servers and PCs to slow down or even crash.

The MultiLink family of switches is capable of detecting and limiting storms on each port. A network administrator can also set the maximum rate of broadcast packets (frames) that are permitted from a particular interface. If the maximum number is exceeded, a storm condition is declared. Once it is determined that a storm is occurring on an interface, any additional broadcast packets received on that interface will be dropped until the storm is determined to be over. The storm is determined to be over when a one-second period elapses with no broadcast packets received.

The `braoadcast-protect` command enables or disables the broadcast storm protection capabilities.

broadcast-protect *<enable|disable>*

The rate-threshold command set the rate limit in frames per second.

rate-threshold *port=<port|list|range> rate=<frames/sec>*

The `show broadcast-protect` command displays the broadcast storm protection settings

show broadcast-protect

In Example 9-3, the broadcast protection is turned on. The threshold for port 11 is then set to a lower value of 3500 broadcast frames/second.

Example 9-3: Preventing broadcast storms

```
ML2400# device
ML2400(device)## show broadcast-protect

=====================================================================
PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
=====================================================================
  9     Disabled    19531                  0                    NO
  10    Disabled    19531                  0                    NO
  11    Disabled    19531                  0                    NO
  12    Disabled    19531                  0                    NO
  13    Disabled    19531                  0                    NO
  14    Disabled    19531                  0                    NO
  15    Disabled    19531                  0                    NO
  16    Disabled    19531                  0                    NO
ML2400(device)## broadcast-protect enable

  Broadcast Storm Protection enabled
ML2400(device)## show broadcast-protect

=====================================================================
PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
=====================================================================
  9     Enabled     19531                  0                    NO
  10    Enabled     19531                  0                    NO
  11    Enabled     19531                  0                    NO
  12    Enabled     19531                  0                    NO
  13    Enabled     19531                  0                    NO
  14    Enabled     19531                  0                    NO
  15    Enabled     19531                  0                    NO
  16    Enabled     19531                  0                    NO
ML2400(device)## rate-threshold port=11 rate=3500

  Broadcast Rate Threshold set
ML2400(device)## show broadcast-protect

=====================================================================
PORT |  STATUS  | THRESHOLD (frms/sec) | CURR RATE (frms/sec) | ACTIVE
=====================================================================
  9     Enabled     19531                  0                    NO
  10    Enabled     19531                  0                    NO
  11    Enabled     3500                   0                    NO
  12    Enabled     19531                  0                    NO
  13    Enabled     19531                  0                    NO
  14    Enabled     19531                  0                    NO
  15    Enabled     19531                  0                    NO
  16    Enabled     19531                  0                    NO
```

9.3.5 Link Loss Alert

The GE Multilin Universal Relay (UR) family and the F650 family of relays have redundant Ethernet ports that allow for automatic switching to their secondary ports when they detect the primary path is broken. The MultiLink switches can compensate for situations where only the switch receiver fiber cable is broken. Upon detection of the broken receiver link, the ML2400 will cease sending link pulses through the relay's receive fiber cable, thereby allowing the relay to switch to its secondary path.

It is recommended to enable the Link Loss Alert (LLA) feature on ports that are connected to end devices. LLA should be disabled for switch ports connected in a ring.

The Link Loss Alert feature is enabled by default on 10 MB Fiber Optic ports, and disabled by default on 100 MB Fiber Optic ports. It can be enabled and disabled via the `lla` parameter in the `setport` command as follows:

setport *port=<port#|list|range> [lla=<enable|disable>]*

The following example illustrates how to enable the link loss alert feature.

Example 9-4: Link loss alert

```
ML2400# device
ML2400(device)## setport port=11 lla=disable
ML2400(device)## show port=11
Configuration details of port 11
-------------------------------------------------
Port Name                       : JohnDoe
Port Link State                 : DOWN
Port Type                       : TP Port
Port Admin State                : Enable
Port VLAN ID                    : 1
Port Speed                      : 10Mbps
Port Duplex Mode                : half-duplex
Port Auto-negotiation State     : Enable
Port STP State                  : NO STP
Port GVRP State                 : No GVRP
Port Priority Type              : None
Port Security                   : Enable
Port Flow Control               : Enable
Port Back Pressure              : Enable
Port Link Loss Alert            : Disable
ML2400(device)## setport port=11 lla=enable
  Link Loss Alert enabled
ML2400(device)## show port=11
Configuration details of port 11
-------------------------------------------------
Port Name                       : JohnDoe
Port Link State                 : DOWN
Port Type                       : TP Port
Port Admin State                : Enable
Port VLAN ID                    : 1
Port Speed                      : 10Mbps
Port Duplex Mode                : half-duplex
Port Auto-negotiation State     : Enable
Port STP State                  : NO STP
Port GVRP State                 : No GVRP
Port Priority Type              : None
Port Security                   : Enable
Port Flow Control               : Enable
Port Back Pressure              : Enable
Port Link Loss Alert            : Enable
```

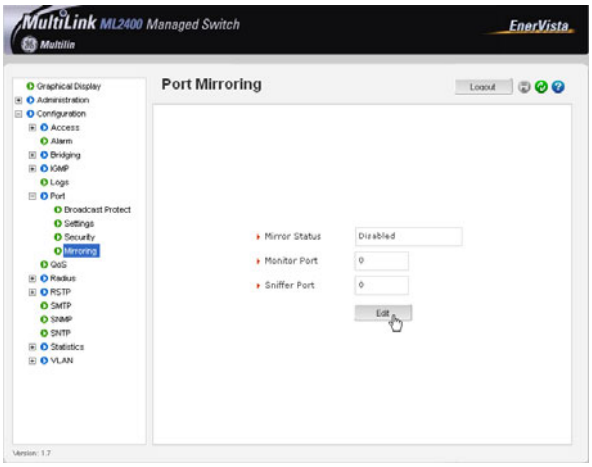
9.4 Port Mirroring using EnerVista Secure Web Management Software

9.4.1 Commands

Monitoring a specific port can be done by port mirroring. Mirroring traffic from one port to another port allows analysis of the traffic on that port.

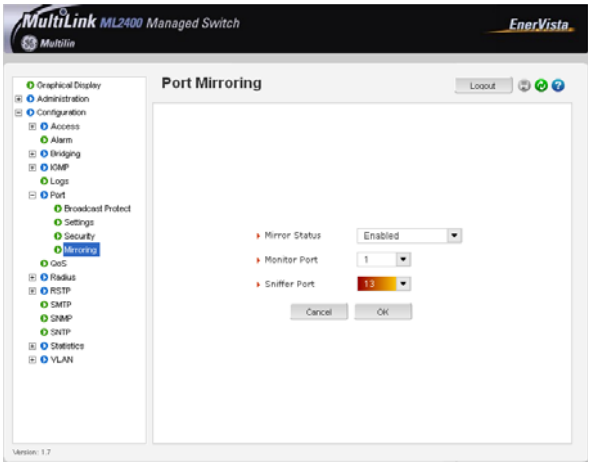
To enable port mirroring as well as setting up the ports to be “sniffed”,

▷ Select the **Configuration > Port > Mirroring** menu item.



▷ Set the sniffer port and the port on which the traffic is reflected.

▷ Make sure the **Mirror Status** is also set to enabled for mirroring:



For security reasons, GE Multilin recommends that the port mirroring be disabled using the **Edit** button and setting the **Mirror Status** to off once port monitoring is completed.

Note that:

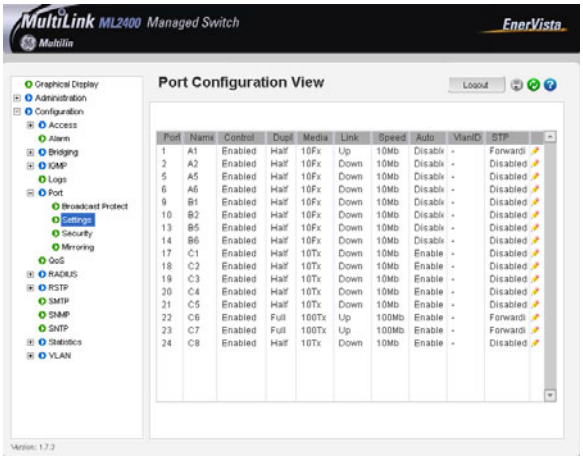
1. Only one port can be set to port mirror at a time.

2. Both the ports (monitored port and mirrored port) have to belong to the same VLAN.
3. The mirrored port shows both incoming as well as outgoing traffic.

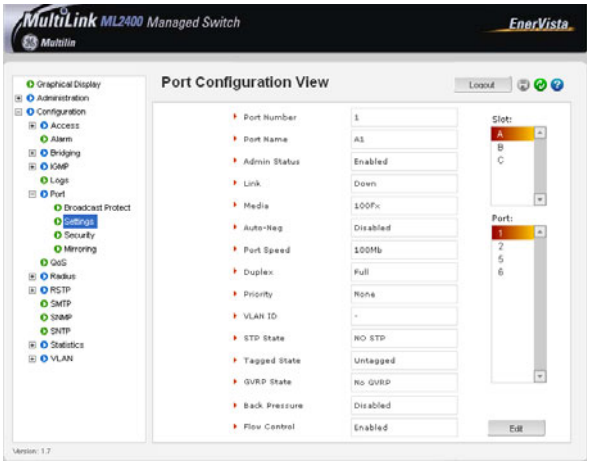
9.4.2 Port Setup

With the ML2400, the specific characteristics of each port can be individually programmed.

▷ Select a specific port by using the edit icon in the **Configuration > Port > Settings** menu.



▷ Click the edit icon to open the following window.



In these windows:

- **Port Number** represents the port number on the switch.
- **Port Name** assigns a specific name to the port. This name is a designated name for the port and can be a server name, user name or any other name.
- **Admin Status** indicates whether the port can be administered remotely.
- **Link** indicates the link status. In the figure above the link is down, implying either there is no connection or the system connected to the port is turned off.

- **Auto-Neg** sets auto negotiation for 100 Mbps and Gigabit copper ports. There is no no auto negotiation for fiber ports as their speeds are fixed.
- The **Port Speed** sets the speed to be 10 or 100 Mbps. This settings works only with 10/100 ports; it is ignored for 10 Mbps ports.
- The **Duplex** setting selects full duplex or half duplex capabilities for 10/100 Mbps ports.
- The **Back Pressure** displays the state of the back pressure setting on the port. This value can be edited in this window.
- The **Flow Control** displays the state of the flow control setting on the port. This value can be edited in this window.
- **Priority** displays the priority set for the port. This value cannot be edited in this window.
- The **VLAN ID** displays the VLAN set for the port. This value cannot be edited in this window.
- The **STP State** displays the STP settings for the port. This value cannot be edited in this window.
- The **Tagged State** displays the Tag settings on the port. This value cannot be edited in this window.
- The **GVRP State** displays the GVRP settings on the port. This value cannot be edited in this window.
- The **LLA** indicates the state of the Link Loss Alert feature.

The "Auto" (default) value for the **Port Speed** senses the speed and negotiates with the port at the other end of the link for data transfer operation (half-duplex or full-duplex). The "Auto" value uses the IEEE 802.3u auto negotiation standard for 100Base-T networks. If the other device does not comply with the 802.3u standard, then the port configuration on the switch must be manually set to match the port configuration on the other device.

Possible port setting combinations for copper ports are:

- 10HDx: 10 Mbps, half-duplex
- 10FDx: 10 Mbps, full-duplex
- 100HDx: 100 Mbps, half-duplex
- 100FDx: 100 Mbps, full-duplex

Possible port settings for 100FX (fiber) ports are:

- 100FDx (default): 100 Mbps, full-duplex
- 100HDx: 100 Mbps, half-duplex

Possible port settings for 10FL (fiber) ports are:

- 10HDx (default): 10 Mbps, half-duplex
- 10FDx: 10 Mbps, full-duplex

Possible port settings for Gigabit fiber-optic ports (Gigabit-SX and Gigabit-LX) are:

- 1000FDx (default): 1000 Mbps (1 GBPS), full duplex only
- Auto: The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port

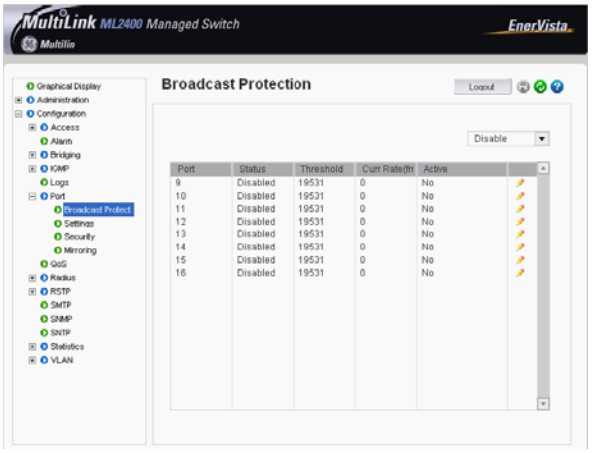
To change the port speed on a transceiver port, the switch must be rebooted

9.4.3 Broadcast Storms

One of the best features of the GE MultiLink switch is its ability to keep broadcast storms from spreading throughout a network. Network storms (or broadcast storms) are characterized by an excessive number of broadcast packets being sent over the network. These storms can occur if network equipment is configured incorrectly or the network software is not properly functioning or badly designed programs (including some network games) are used. Storms can reduce network performance and cause bridges, routers, workstations, servers and PCs to slow down or even crash.

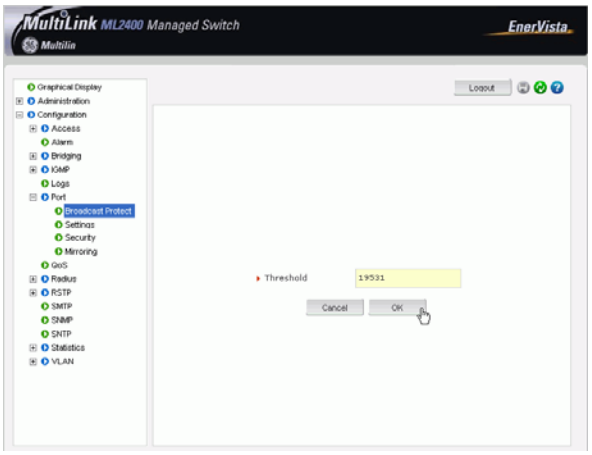
The GE MultiLink switch is capable of detecting and limiting storms on each port. A network administrator can also set the maximum rate of broadcast packets (frames) that are permitted from a particular interface. If the maximum number is exceeded, a storm condition is declared. Once it is determined that a storm is occurring on an interface, any additional broadcast packets received on that interface will be dropped until the storm is determined to be over. The storm is determined to be over when a one-second period elapses with no broadcast packets received.

Broadcast storm protection can be configured through the **Configuration > Port > Broadcast Storm** menu.



▷ **To edit the threshold level, click on the edit icon as seen below.**

See details in *Broadcast Storms* on page 9–8 to determine the threshold level.



▷ After changes are made, **do not forget** to save the changes using the save icon ( ).
If the switch is rebooted before the changes are made, the changes will be lost.

Multilink ML2400

Ethernet Communications Switch

Chapter 10: VLAN

10.1 VLAN Description

10.1.1 Overview

Short for virtual LAN (VLAN), a VLAN creates separate collision domains or network segments that can span multiple MultiLink switches. A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. The IEEE 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames.

VLANs provide the capability of having two (or more) Ethernet segments co-exist on common hardware. The reason for creating multiple segments in Ethernet is to isolate collision domains. VLANs can isolate groups of users, or divide up traffic for security, bandwidth management, etc. VLANs are widely used today and are here to stay. VLANs need not be in one physical location. They can be spread across geography or topology. VLAN membership information can be propagated across multiple MultiLink switches.

The following figure illustrates a VLAN as two separate collision domains. The top part of the figure shows two "traditional" Ethernet segments. Up to 32 VLANs can be defined per switch.

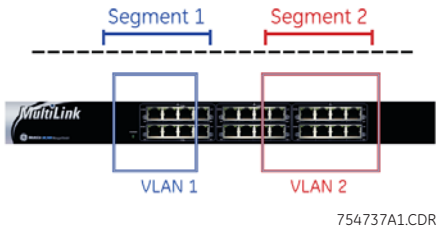
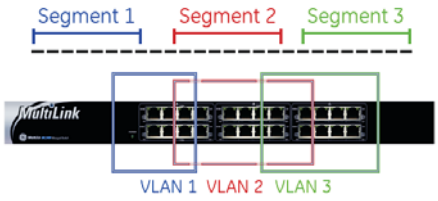


FIGURE 10–1: VLAN as two separate collision domains

A group of network users (ports) assigned to a VLAN form a broadcast domain. Packets are forwarded only between ports that are designated for the same VLAN. Cross-domain broadcast traffic in the switch is eliminated and bandwidth is saved by not allowing packets to flood out on all ports. For many reasons a port may be configured to belong to multiple VLANs.

As shown below, ports can belong to multiple VLANs. In this figure, a simplistic view is presented where some ports belong to VLANs 1, 2 and other ports belong to VLANs 2,3. Ports can belong to VLANs 1, 2 and 3. This is not shown in the figure.



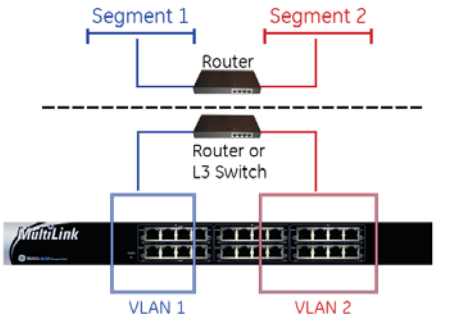
754738A1.CDR

FIGURE 10–2: Ports assigned to multiple VLANs

By default, on the MultiLink family of switches, VLAN support is enabled and all ports on the switch belong to the default VLAN (DEFAULT-VLAN). This places all ports on the switch into one physical broadcast domain.

If VLANs are entirely separate segments or traffic domains - how can the VLANs route traffic (or "talk") to each other? This can be done using routing technologies (e.g., a router or a L3-switch). The routing function can be done internally to a L3-switch. One advantage of an L3 switch is that the switch can also support multiple VLANs. The L3 switch can thus route traffic across multiple VLANs easily and provides a cost effective solution if there are may VLANs defined.

As shown below, routing between different VLANs is performed using a router or a Layer 3 switch (L3-switch)



754739A1.CDR

FIGURE 10–3: VLAN routing

The MultiLink family of switches supports up to 32 VLANs per switch

10.1.2 Tag VLAN vs. Port VLAN

What is the difference between tag and port VLAN? In a nutshell - port VLAN sets a specific port or group of ports to belong to a VLAN. Port VLANs do not look for VLAN identifier (VID) information nor does it manipulate the VID information. It thus works “transparently” and propagates the VLAN information along.

In the tag VLAN, an identifier called the VLAN identifier (VID) is either inserted or manipulated. This manipulated VLAN tag allows VLAN information to be propagated across devices or switches, allowing VLAN information to span multiple switches.

As described earlier, VLAN is an administratively configured LAN or broadcast domain. Instead of going to the wiring closet to move a cable to a different LAN segment, the same task can be accomplished remotely by configuring a port on an 802.1Q-compliant switch to belong to a different VLAN. The ability to move end stations to different broadcast domains by setting membership profiles for each port on centrally managed switches is one of the main advantages of 802.1Q VLANs.

802.1Q VLANs aren't limited to one switch. VLANs can span many switches. Sharing VLANs between switches is achieved by inserting a tag with a VLAN identifier (VID) into each frame. A VID must be assigned for each VLAN. By assigning the same VID to VLANs on many switches, one or more VLAN (broadcast domain) can be extended across a large network.

802.1Q-compliant switch ports, such as those on the MultiLink family of switches, can be configured to transmit tagged or untagged frames. A tag field containing VLAN information can be inserted into an Ethernet frame. If a port has an 802.1Q-compliant device attached (such as another switch), these tagged frames can carry VLAN membership information between switches, thus letting a VLAN span multiple switches. Normally connections between switches can carry multiple VLAN information and this is call port trunking or 802.1Q trunks.

There is one important caveat: administrators must ensure ports with non-802.1Q-compliant devices attached are configured to transmit untagged frames. Many network interface cards such as those for PCs printers and other “dumb” switches are not 802.1Q-compliant. If they receive a tagged frame, they will not understand the VLAN tag and will drop the frame. In situations like these, its best to use port based VLANs for connecting to these devices.

Sometimes a port may want to listen to broadcasts across different VLANs or propagate the VLAN information on to other ports. This port must thus belong to multiple VLANs so that the broadcast information reaches the port accurately. If the port also wants to send broadcast traffic, the proper leave (sending out of information) and join rules (receiving information) have to be configured on the MultiLink family of switches.

It is recommended to use IEEE 802.1q tagged based VLANs over port based VLANs because of there multi-vendor interoperability and capability of carrying the isolated tagged VLAN information when more than one switch is involved.

10.2 Configuring Port VLANs through the Command Line Interface

10.2.1 Description

Port VLANs are rarely used in networks which use VLANs across multiple switches. Port VLANs are used when VLANs are setup up on a single switch and connectivity between the system on different VLANs is needed however the broadcasts and multicasts are isolated to the specific VLAN.

GE recommends using the set-port command for setting the port based VLAN as well.

General steps for using port VLANs are

1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs.
2. Configure at least one VLAN in addition to the default VLAN
3. Assign the desired ports to the VLANs
4. Decide on trunking strategy - how will the VLAN information be propagated from one switch to another and also what VLAN information will be propagated across
5. (Layer 3 consideration) check to see if the routing between the VLANs is "working" by pinging stations on different VLANs

You can rename the default VLAN, but you cannot change its VID (1) or delete it from the switch

Any ports not specifically assigned to another VLAN will remain assigned to the DEFAULT-VLAN

Changing the number of VLANs supported on the switch requires the SAVE command to save the new VLAN information

10.2.2 Commands

The following commands are used for VLANs. To define the VLAN type:

set vlan *type=<port|tag|none>*

To configure a VLAN:

configure vlan *type=port*
vlan *type=port*

To add VLANs:

add *id=<vlan Id> [name=<vlan name>] port=<number|list|range>*

To start VLANs:

start *vlan=<name|number|list|range>*

To save VLAN configuration:

save

To edit VLANs:

edit *id=<vlan Id> [name=<vlan name>] port=<number|list|range>*

To display the VLAN information:

show vlan *type=<port|tag> [<id=vlanid>]*

The following command sequence shows how to configure VLANs on a MultiLink switch.

ML2400# `vlan type=port`

ML2400(port-vlan)## `add id=2 name=test port=1-10`

ML2400(port-vlan)## `start vlan=all`

ML2400(port-vlan)## `save`

```
Saving current configuration...
Configuration saved
```

To move Management Control on any VLAN:

add *id=<vlan Id> [name=<vlan name>] port=<number|list|range> [Forbid=<number|list|range>]****[<mgt|nomgt>]***

To enable or disable Management Control on any VLAN:

*edit id=<vlan Id>[name=<vlan name>][port=<number|list|range>****[<mgt|nomgt>]***

10.2.3 Example

Example 10-1 below shows how to add three different VLANs. Along with the VLANs, Port 14 is assigned to the four VLANs - the three new ones added plus the DEFAULT-VLAN 1. The following interaction shows how VLANs 10, 20, 30 are added to port 14 and the VLANs activated. A typical use for such a port would be to connect a “dumb” switch to this port and allow traffic from three different VLANs to pass through transparently to the “dumb” switch, which will be connected to port 14. Note in this example, VLAN information is not propagated on to the “dumb” switch.

Example 10-1: Adding three VLANs

```
ML2400# set vlan type=port
  VLAN set to Port-based.
ML2400# vlan type=port
ML2400(port-vlan)## add id=10 name=engineering port=14
Vlan added successfully with
  Vlan id      : 10
  Vlan name    : engineering
  Ports        : 14
ML2400(port-vlan)## add id=20 name=engineering port=14
  ERROR - Duplicate Vlan name
ML2400(port-vlan)## add id=20 name=sales port=14
Vlan added successfully with
  Vlan id      : 20
  Vlan name    : sales
  Ports        : 14
ML2400(port-vlan)## add id=30 name=marketing port=14
Vlan added successfully with
  Vlan id      : 30
  Vlan name    : marketing
  Ports        : 14
```

Each VLAN requires a unique name. Here, VLAN 10 and 20 had the same name

(continued on next page)

Adding three VLANs (continued)

ML2400(port-vlan)## `show vlan type=port`

```
VLAN ID    : 1
Name       : Default VLAN
Status     : Active

========================
  PORT   |       STATUS
========================
     9   |       UP
    10   |       DOWN
    11   |       DOWN
    12   |       DOWN
    13   |       UP
    14   |       DOWN
    15   |       DOWN
    16   |       DOWN

VLAN ID    : 10
Name       : engineering
Status     : Pending
========================
  PORT   |       STATUS
========================
    14   |       DOWN

VLAN ID    : 20
Name       : sales
Status     : Pending
========================
  PORT   |       STATUS
========================
    14   |       DOWN

VLAN ID    : 30
Name       : marketing
Status     : Pending
========================
  PORT   |       STATUS
========================
    14   |       DOWN
```

The added VLANs are not yet active. Each individual VLAN can be activated or all VLANs can be activated.

Start all VLANs

ML2400(port-vlan)## `start vlan=all`

```
All pending VLAN's started.
```

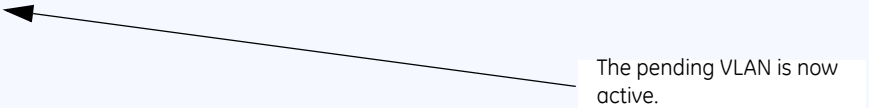
ML2400(port-vlan)## `show vlan type=port`

```
VLAN ID    : 1
Name       : Default VLAN
Status     : Active

========================
  PORT   |       STATUS
========================
     9   |       UP
    10   |       DOWN
    11   |       DOWN
    12   |       DOWN
    13   |       UP
    14   |       DOWN
    15   |       DOWN
    16   |       DOWN
```

(continued on next page)

Adding three VLANs (continued)

```
VLAN ID    : 10
Name       : engineering
Status     : Active
========================
  PORT   |        STATUS
========================
    14   |        DOWN

VLAN ID    : 20
Name       : sales
Status     : Active
========================
  PORT   |        STATUS
========================
    14   |        DOWN

VLAN ID    : 30
Name       : markteting
Status     : Active
========================
  PORT   |        STATUS
========================
    14   |        DOWN
```



ML2400(port-vlan)## exit

ML2400#

10.3 Configuring Port VLANs with EnerVista Secure Web Management Software

10.3.1 Description

Port VLANs are rarely used in networks which use VLANs across multiple switches. Port VLANs are used when VLANs are setup up on a single switch and connectivity between the systems on different VLANs is needed; however, the broadcasts and multicasts are isolated to the specific VLAN.

Either port VLANs or Tag VLAN can be active at any given time on a switch. Only the default VLAN (VLAN ID = 1) is active as a Tag VLAN as well as a port VLAN.

General steps for using port VLANs are

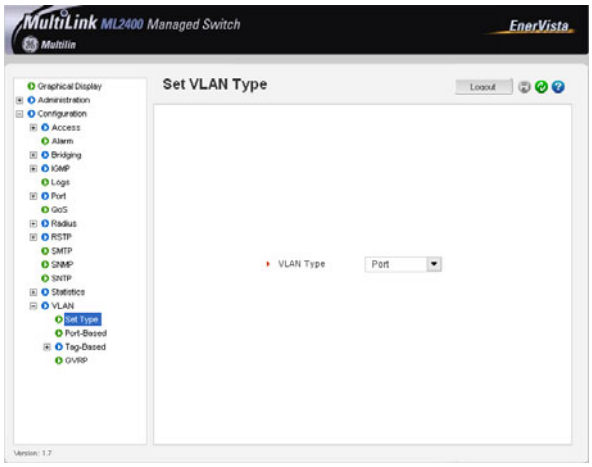
1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs.
2. Configure at least one VLAN in addition to the default VLAN.
3. Assign the desired ports to the VLANs
4. Decide on trunking strategy – how will the VLAN information be propagated from one switch to another and also what VLAN information will be propagated across.
5. Layer 3 consideration – check to see if the routing between the VLANs is "working" by pinging stations on different VLANs

You can rename the default VLAN, but you cannot change its VID =1 or delete it from the switch.

Any ports not specifically assigned to another VLAN will remain assigned to the DEFAULT-VLAN (VID=1).

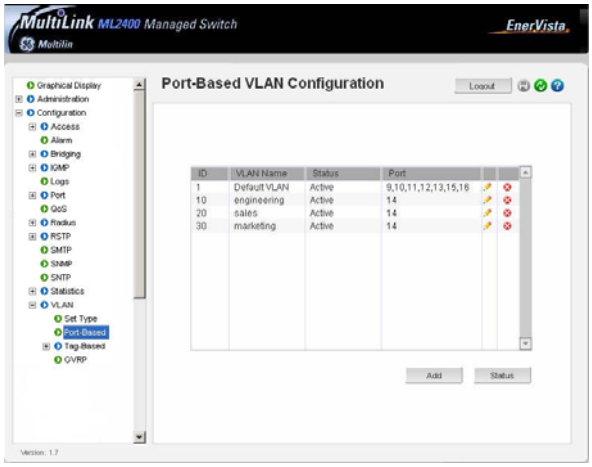
Changing the number of VLANs supported on the switch requires the changes to be saved for future use. To eliminate the changes, reboot the switch without saving the changes.

For VLAN configuration use **Configuration > VLAN** menu items as shown below. The Port VLANs are active by default.

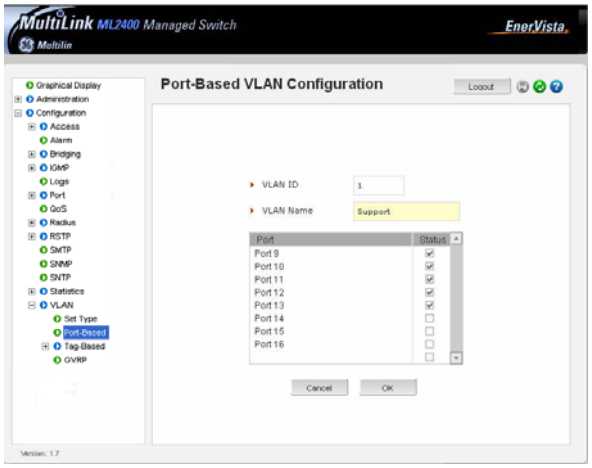


The currently assigned Port VLANs are displayed as follows:

▷ Select the **Configuration > VLAN > Port-Based** menu item.



As discussed above, ports 9, 10, 11, 12, 13, 15, 16 still belong to default VLAN. We will now add another VLAN with VID=40 and VLAN name = Support.

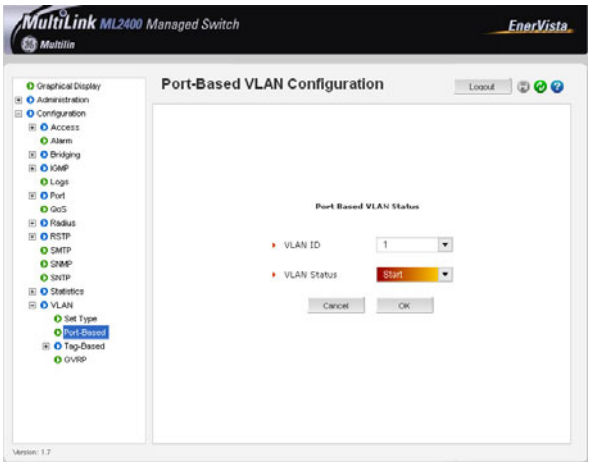


▷ Add the ports.

▷ Define the VLAN.

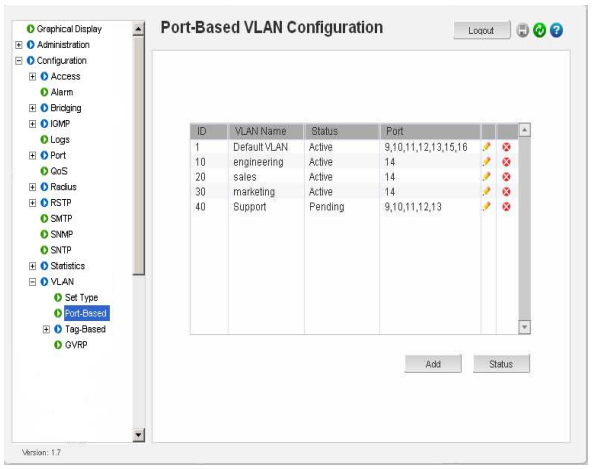
▷ Click OK.

.



After adding the VLAN, the VLAN is not active. Activating the VLAN has to be done manually.

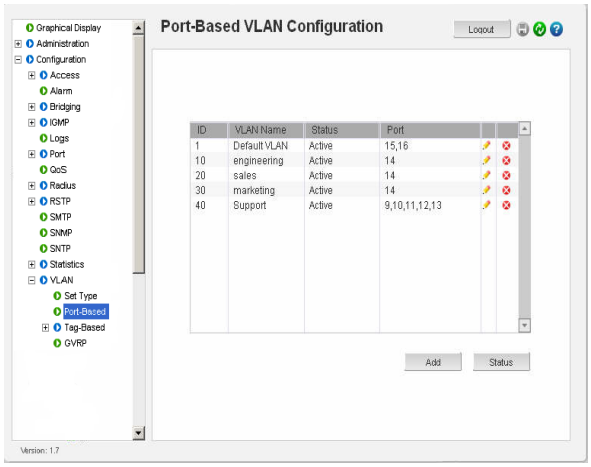
▷ To activate the VLAN, click on the **Status** button..



A specific VLAN can be activated or all VLANs can be activated (or disabled).

▷ Click **OK** to activate VLAN.

.



After activation, note that ports 9 to 13 belong to the new VLAN. Their membership in the default VLAN has been eliminated.

Note the VLAN membership of the ports assigned to VLAN 40 now indicates that they are only members of VLAN 40. The default VLAN membership has been terminated on VLAN activation. The ports can be added to VLAN 1 by using the edit button on VLAN 1 and assigning the ports to VLAN 1.

10.4 Configuring Tag VLANs through the Command Line Interface

10.4.1 Description

The VLAN information needs to be propagated on to other switches when multiple switches are connected on a network. In these situations it is best to use tag-based VLANs.

NOTE

For versions 1.6.1 and below, the use of tag VLANs needed the `set-ingress` and `set-egress` commands to set the flow of incoming and outgoing traffic. These commands are defunct as of MultiLink Switch Software version 1.6.1. For legacy purposes, these commands will still work with release 1.6.1 (and will print a message on the screen indicating the commands are deprecated), however, GE strongly recommends avoiding these commands and using the `set-port` command instead.

10.4.2 Commands

The `set-port` command for setting Tag VLANs has the following parameters. The `default id` parameter sets the default VLAN id (termed PVID in previous versions). The default VLAN id is the VLAN id assigned to the untagged packets received on that port. For Multilink family of switches, the default VLAN id is 1

set-port *port=<number|list|range>*
default id=<number>

The `filter` parameter enables or disables the VLAN filtering function. When enabled, the switch will drop the packets coming in through a port if the port is not a member of the VLAN. For example, if port 1 is a member of VLANs 10, 20 and 30, if a packet with VLAN id 40 arrives at port 1 it will be dropped.

set-port *port=<number|list|range>*
filter status=<enable|disable>

The `tagging id` and `status` parameters define whether the outgoing packets from a port will be tagged or untagged. This definition is on a per VLAN basis. For example, the command `set-port port=1 tagging id=10 status=tagged` will instruct the switch to tag all packets going out of port 1 to belong to VLAN 10.

set-port *port=<number|list|range>*
tagging id=<number> status=<tagged|untagged>

The `join id` parameter adds the specified port(s) to the specified VLAN id. This parameter works with active or pending VLANs.

set-port *port=<number|list|range>*
join id=<number>

The `leave id` parameter releases a specific port from a VLAN. For example if port 1 belongs to VLAN 10, 20, 30, 40 the command set-port port=1 leave id=40 makes port 1 belong to VLAN 10, 20, 30, dropping VLAN 40.

set-port *port=<number|list|range>*
leave id=<number>

The `show-port` command lists all parameters related to tag VLAN for the list of ports. If the `port` parameter is omitted, it will display all ports.

show-port [port=<port|list|range>]

To move Management Control on any VLAN:

add *id=<vlan Id> [name=<vlan name>] port=<number|list|range> [Forbid=<number|list|range>]****[<mgt|nomgt>]***

To enable or disable Management Control on any VLAN:

*edit id=<vlan Id>[name=<vlan name>][port=<number|list|range>****[<mgt|nomgt>]***

10.4.3 Example

In the following example, we start with Port VLAN and convert to TAG VLAN. We define ports 14 through 16 to belong to VLANs 10, 20 and 30 and the rest of the ports belong to the default VLAN (in this case, VLAN 1). Filtering is enabled on ports 14-16. The VLAN setup is done before devices are plugged into ports 14-16 as a result the status of the ports show the port status as DOWN.

1. A word of caution - when Tag VLAN filtering is enabled, there can be serious connectivity repercussions - the only way to recover from that it is to reload the switch without saving the configuration or by modifying the configuration from the console (serial) port.
2. There can be either Tag VLAN or Port VLAN. Both VLANs cannot co-exit at the same time.
3. There can only be one default VLAN for the switch. The default is set to VLAN 1 and can be changed to another VLAN. A word of caution on changing the default VLAN as well - there can be repercussions on management as well as multicast and other issues.
4. Tag VLAN support VLAN ids from 1 to 4096. VLAN ids more than 2048 are reserved for specific purposes and it is recommended they not be used.

Example 10-2: Converting Port VLAN to Tag VLAN

```
ML2400# vlan type=port
ML2400(port-vlan)## show vlan type=port
  VLAN ID    : 1
  Name       : Default VLAN
  Status     : Active

  ========================
    PORT   |       STATUS
  ========================
       9   |       UP
      10   |       DOWN
      11   |       DOWN
      12   |       DOWN
      13   |       UP
      14   |       DOWN
      15   |       DOWN
      16   |       DOWN

  VLAN ID    : 10
  Name       : engineering
  Status     : Active

  ========================
    PORT   |       STATUS
  ========================
      14   |       DOWN

  VLAN ID    : 20
  Name       : sales
  Status     : Active

  ========================
    PORT   |       STATUS
  ========================
      14   |       DOWN

  VLAN ID    : 30
  Name       : markteting
  Status     : Active

  ========================
    PORT   |       STATUS
  ========================
      14   |       DOWN
ML2400(port-vlan)## stop vlan=all
  All active VLAN's stopped.
ML2400(port-vlan)## exit
ML2400# set vlan type=tag
  VLAN set to Tag-based.
ML2400# show active-vlan
Tag VLAN is currently active.
```

To switch to Tag VLAN, the port VLAN has to be disabled or stopped. Only one type of VLAN can co-exist at the same time. Exit out of Port VLAN configuration mode and set the VLAN type to be Tag VLAN.

(continued on next page)

Converting Port VLAN to Tag VLAN (continued)

```
ML2400# show vlan type=tag

  VLAN ID    : 1
  Name       : Default VLAN
  Status     : Active

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
       9   |  UNTAGGED   |  UP
      10   |  UNTAGGED   |  DOWN
      11   |  UNTAGGED   |  DOWN
      12   |  UNTAGGED   |  DOWN
      13   |  UNTAGGED   |  UP
      14   |  UNTAGGED   |  DOWN
      15   |  UNTAGGED   |  DOWN
      16   |  UNTAGGED   |  DOWN
```

Note that ports 14 to 16 are "DOWN" - the VLAN configuration is preferably done before devices are plugged in to avoid connectivity repercussions.

```
ML2400# vlan type=tag
ML2400(tag-vlan)## add id=10 name=mkt port=14-16

  Tag based vlan Added Successfully.
  VLAN ID      : 10
  VLAN Name    : mkt
  Ports        : 14-16
ML2400(tag-vlan)## edit id=10 name=engineering port=14-16

  Tag based vlan Added Successfully.
  VLAN ID      : 10
  VLAN Name    : engineering
  Ports        : 14-16
ML2400(tag-vlan)## add id=20 name=sales port=14-16

  Tag based vlan Added Successfully.
  VLAN ID      : 20
  VLAN Name    : sales
  Ports        : 14-16
ML2400(tag-vlan)## add id=20 name=marketing port=14-16

  ERROR: Duplicate Vlan Id
```

Intentionally executed to show the effect of adding a duplicate VLAN.

```
ML2400(tag-vlan)## add id=30 name=marketing port=14-16

  Tag based vlan Added Successfully.
  VLAN ID      : 30
  VLAN Name    : marketing
  Ports        : 14-16
```

(continued on next page)

Converting Port VLAN to Tag VLAN (continued)

```
ML2400(tag-vlan)## show vlan type=tag

  VLAN ID    : 1
  Name       : Default VLAN
  Status     : Active

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
       9   |  UNTAGGED   |  UP
      10   |  UNTAGGED   |  DOWN
      11   |  UNTAGGED   |  DOWN
      12   |  UNTAGGED   |  DOWN
      13   |  UNTAGGED   |  UP
      14   |  UNTAGGED   |  DOWN
      15   |  UNTAGGED   |  DOWN
      16   |  UNTAGGED   |  DOWN

  VLAN ID    : 10
  Name       : engineering
  Status     : Pending

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
      14   |  UNTAGGED   |  DOWN
      15   |  UNTAGGED   |  DOWN
      16   |  UNTAGGED   |  DOWN

  VLAN ID    : 20
  Name       : sales
  Status     : Pending

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
      14   |  UNTAGGED   |  DOWN
      15   |  UNTAGGED   |  DOWN
      16   |  UNTAGGED   |  DOWN

  VLAN ID    : 30
  Name       : marketing
  Status     : Pending

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
      14   |  UNTAGGED   |  DOWN
      15   |  UNTAGGED   |  DOWN
      16   |  UNTAGGED   |  DOWN
ML2400(tag-vlan)## start vlan=all

  All pending VLAN's started.
```

Note that the VLANs are not started as yet. Adding the VLAN does not start it by default.

(continued on next page)

Converting Port VLAN to Tag VLAN (continued)

```
ML2400(tag-vlan)## set-port port=14-16 filter status=enable

  WARNING: PVID does not match the port(15)'s VLAN ID(s).
  If you are using telnet session on this port,setting ingress might stop the session.

  Do you want to continue? ['Y' or 'N'] Y

  WARNING: PVID does not match the port(14)'s VLAN ID(s).
  If you are using telnet session on this port, setting ingress might stop the session.

  Do you want to continue? ['Y' or 'N'] Y

  WARNING: PVID does not match the port(16)'s VLAN ID(s).
  If you are using telnet session on this port, setting ingress might stop the session.

  Do you want to continue? ['Y' or 'N'] Y

Ingress Filter Enabled
```

Enable filtering on the ports required. The software will prompt to ensure that connectivity is not disrupted.

```
ML2400(tag-vlan)## show vlan type=tag

  VLAN ID    : 1
  Name       : Default VLAN
  Status     : Active

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
       9   |  UNTAGGED   |  UP
      10   |  UNTAGGED   |  DOWN
      11   |  UNTAGGED   |  DOWN
      12   |  UNTAGGED   |  DOWN
      13   |  UNTAGGED   |  UP

  VLAN ID    : 10
  Name       : engineering
  Status     : Active

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
      14   |  UNTAGGED   |  DOWN
      15   |  UNTAGGED   |  DOWN
      16   |  UNTAGGED   |  DOWN

  VLAN ID    : 20
  Name       : sales
  Status     : Active

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
      14   |  UNTAGGED   |  DOWN
      15   |  UNTAGGED   |  DOWN
      16   |  UNTAGGED   |  DOWN

  VLAN ID    : 30
  Name       : marketing
  Status     : Active

  ==============================
    PORT   |  MODE       |  STATUS
  ==============================
      14   |  UNTAGGED   |  DOWN
      15   |  UNTAGGED   |  DOWN
      16   |  UNTAGGED   |  DOWN
```

VLANs are now active. However, as the packet traverses VLANs, the packet should be tagged. This is enabled next.

(continued on next page)

Converting Port VLAN to Tag VLAN (continued)

```
ML2400(tag-vlan)## set-port port=14-16 tagging id=10 status=tagged
  Port tagging enabled
ML2400(tag-vlan)## set-port port=14-16 tagging id=20 status=tagged
  Port tagging enabled
ML2400(tag-vlan)## set-port port=14-16 tagging id=30 status=tagged
  Port tagging enabled
ML2400(tag-vlan)## show vlan type=tag
  VLAN ID   : 1
  Name      : Default VLAN
  Status    : Active

  ==============================
    PORT   |  MODE      |  STATUS
  ==============================
       9   |  UNTAGGED  |  UP
      10   |  UNTAGGED  |  DOWN
      11   |  UNTAGGED  |  DOWN
      12   |  UNTAGGED  |  DOWN
      13   |  UNTAGGED  |  UP

  VLAN ID   : 10
  Name      : engineering
  Status    : Active

  ==============================
    PORT   |  MODE      |  STATUS
  ==============================
      14   |  TAGGED    |  DOWN
      15   |  TAGGED    |  DOWN
      16   |  TAGGED    |  DOWN

  VLAN ID   : 20
  Name      : sales
  Status    : Active

  ==============================
    PORT   |  MODE      |  STATUS
  ==============================
      14   |  TAGGED    |  DOWN
      15   |  TAGGED    |  DOWN
      16   |  TAGGED    |  DOWN

  VLAN ID   : 30
  Name      : marketing
  Status    : Active

  ==============================
    PORT   |  MODE      |  STATUS
  ==============================
      14   |  TAGGED    |  DOWN
      15   |  TAGGED    |  DOWN
      16   |  TAGGED    |  DOWN
```

10.5 Configuring Tag VLANs with EnerVista Secure Web Management Software

10.5.1 Description

When multiple switches are on a network, the VLAN information needs to be propagated on to other switches. In such situations, it is best to use tag based VLANs.

On the MultiLink ML2400 Ethernet Switch, the port VLAN type is set to none. To use Tag VLANs, first enable Tag VLANs.

In the following example, we assign various ports as VLANs 10, 20 and 30 and the remaining ports to the default VLAN (that is, VLAN 1).

The VLAN setup occurs before devices are connected to the ports. As such, the port status is shown as DOWN.

CAUTION

There can be serious connectivity repercussions when Tag VLAN filtering is enabled. The only way to recover from this it is to reload the switch without saving the configuration or by modifying the configuration from the console (serial) port.

The ML2400 can be configured for either Tag VLAN or Port VLAN. Both VLANs cannot co-exit at the same time. There can only be one default VLAN for the switch. The default is set to VLAN 1 and can be changed to another VLAN.

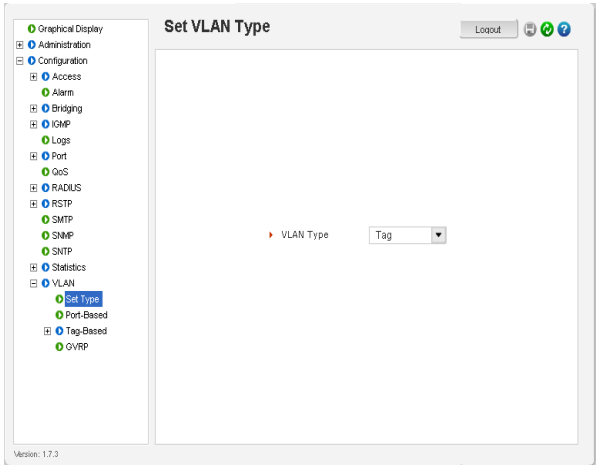
CAUTION

There can be repercussions on management as well as multicast and other issues when changing the default VLAN.

Tag VLAN supports VLAN IDs from 1 to 4096. VLAN IDs greater than 2048 are reserved for specific purposes. As such, it is recommended they not be used.

To use the Tag VLAN, first

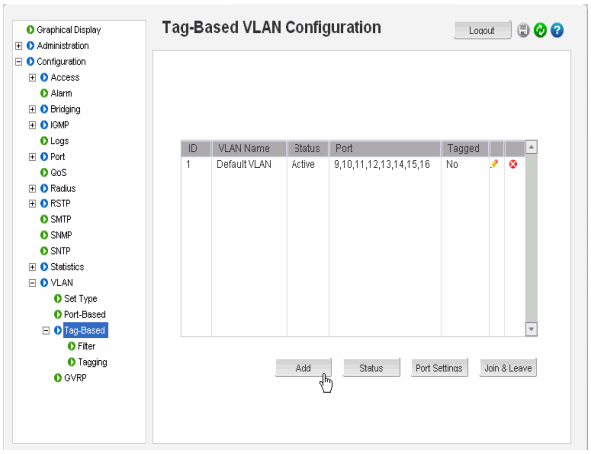
▷ Set the VLAN type to Tag in the **Configuration > VLAN > Set Type** menu.



The next step is to define the VLANs needed. To do that,

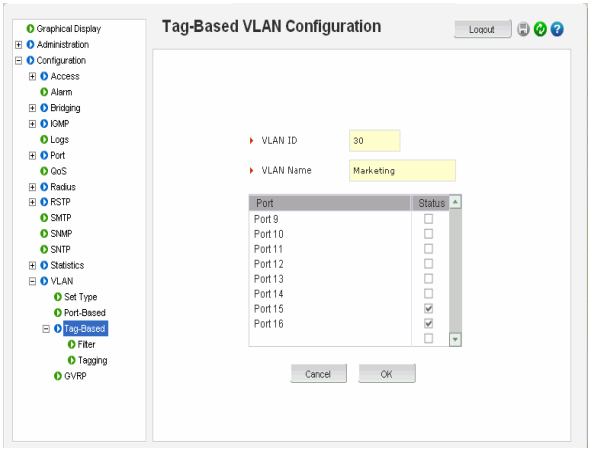
▷ Click On **Configuration >vlan >tag-based** Menu.

▷ Click on the **Add** button.



▷ Now add the necessary VLANs.
In the example below, add the VLANs in the following manner

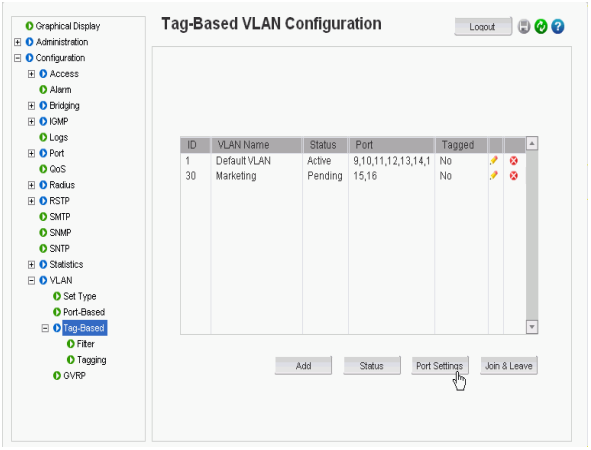
- VLAN 1, All ports - default VLAN
- VLAN 10, Engineering VLAN - ports 11, 12, 13
- VLAN 20, Support VLAN - ports 13, 14, 15 (note that port 13 belongs to VLAN 10, 20)
- VLAN 30, Marketing VLAN -ports 15, 16 (note that port 15 belongs to VLAN 20, 30)

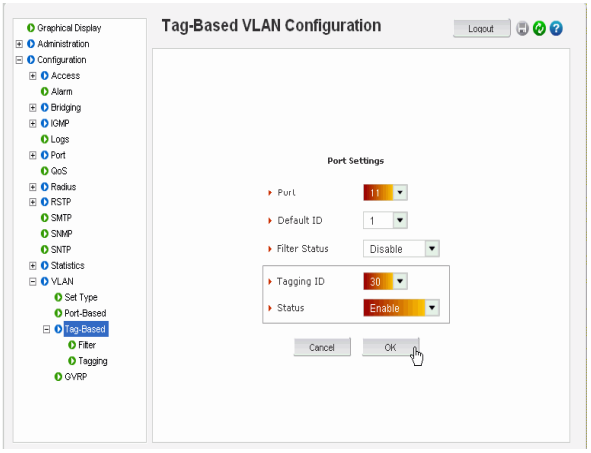


▷ After adding the ports and defining the VLAN, click **OK**.

▷ Click on **Port Settings** in the **Configuration >VLAN >Tag-Based** menu and enable the tagging for each port.

.



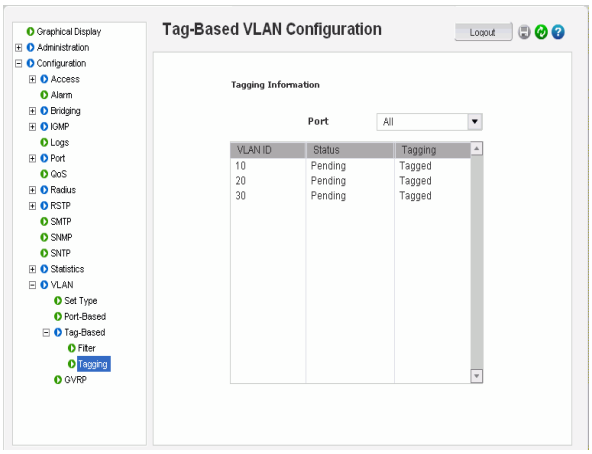


▷ Repeat the last two steps for each of the ports and each of the VLANs (click on port settings and enable the tag on the port.) After all the ports are tagged, the tagged column should change to "Yes" for all VLANs

To check the status of the tagging,

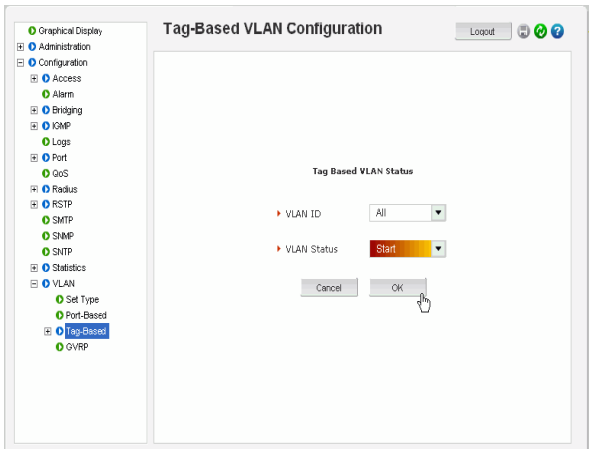
▷ Select the **Configuration > VLAN > Tag-Based > Tagging** menu.

.



To activate the VLAN,

- ▷ Click on the Status button under the **Configuration >VLAN >Tag-Based > Settings** menu.
- ▷ Click OK.

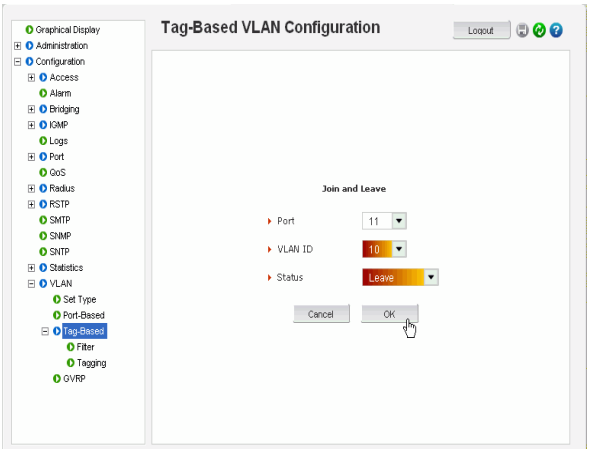


Tagged VLANs can be viewed from the **Configuration > VLAN > Tag-Based > Tagging** menu.

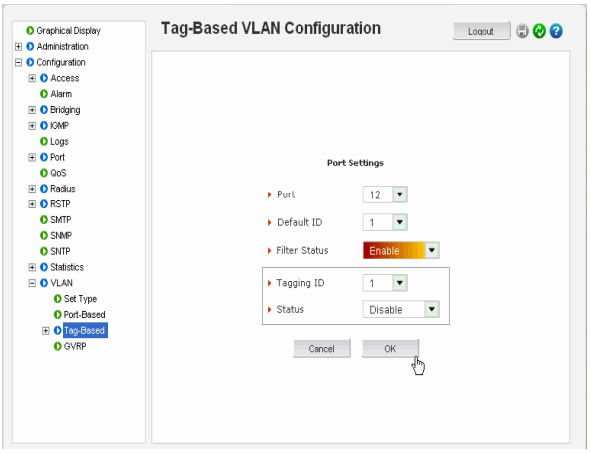
To add or delete specific ports from a VLAN,

- ▷ Click on **Join & Leave** button from the **Configuration > VLAN >. Tag-Based > Settings** menu and specify the action.
  In the example below, we will take port 11 and assign it to leave VLAN 10. After the action is completed, note that port 11 will belong to VLAN 1 only.

.



To enable the filter capability for each port, use the **Configuration >VLAN >Tag-Based > Settings** menu as shown below.



Use the **Configuration >VLAN >Tag-Based > Filter** menu to view the filter information for the ports.

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 11: VLAN Registration over GARP

11.1 Overview

11.1.1 Description

The Generic Attribute Registration Protocol (GARP) and VLAN registration over GARP is called GVRP. GVRP is defined in the IEEE 802.1q and GARP in the IEEE 802.1p standards. To utilize the capabilities of GVRP, GE Multilin recommends that the user become familiar with the concepts and capabilities of IEEE 802.1q.

11.1.2 GVRP Concepts

GVRP makes it easy to propagate VLAN information across multiple switches. Without GVRP, a network administrator has to go to each individual switch and enable the necessary VLAN information or block specific VLANs so that the network integrity is maintained. With GVRP, this process can be automated.

It is critical that all switches share a common VLAN. This VLAN typically is the default VLAN (VID=1) on most switches and other devices. GVRP uses "GVRP Bridge Protocol Data Units" ("GVRP BPDUs") to "advertise" static VLANs. We refer to GVRP BPDU is as an "advertisement".

GVRP enables the MultiLink family of switches to dynamically create 802.1q-compliant VLANs on links with other devices running GVRP. This enables the switch to automatically create VLAN links between GVRP-aware devices. A GVRP link can include intermediate devices that are not GVRP-aware. This operation reduces the chances for errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. GVRP can thus be used to propagate VLANs to other GVRP-aware devices instead of manually having to set up VLANs across the network. After the switch creates a dynamic VLAN, GVRP can also be used to dynamically enable port membership in static VLANs configured on a switch.

NOTE

There must be one common VLAN (that is, one common VID) connecting all of the GVRP-aware devices in the network to carry GVRP packets. GE Multilin recommends the default VLAN (DEFAULT_VLAN; VID = 1), which is automatically enabled and configured as untagged on every port of the MultiLink family of switches. That is, on ports used as GVRP links, leave the default VLAN set to untagged and configure other static VLANs on the ports as either "Tagged or Forbid" ("Forbid" is discussed later in this chapter).

11.1.3 GVRP Operations

A GVRP-enabled port with a tagged or untagged static VLAN sends advertisements (BPDUs, or Bridge Protocol Data Units) advertising the VLAN identification (VID) Another GVRP-aware port receiving the advertisements over a link can dynamically join the advertised VLAN. All dynamic VLANs operate as Tagged VLANs. Also, a GVRP-enabled port can forward an advertisement for a VLAN it learned about from other ports on the same switch. However, the forwarding port will not itself join that VLAN until an advertisement for that VLAN is received on that specific port.

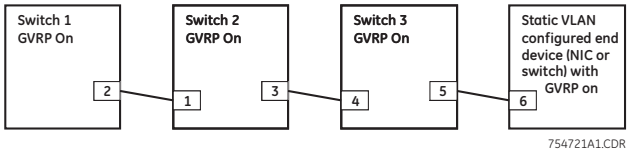


FIGURE 11–1: GVRP operation

Switch 1 with static VLANs (VID= 1, 2, and 3). Port 2 is a member of VIDs 1, 2, and 3.

1. Port 2 advertises VIDs 1, 2, and 3.
2. On Switch 2 - Port 1 receives advertisement of VIDs 1, 2, and 3 AND becomes a member of VIDs 1, 2, and 3.
3. As discussed above, a GVRP enabled port can forward advertisement for a VLAN it learnt about. So port 3 advertises VIDs 1, 2, and 3, but port 3 is NOT a member of VIDs 1, 2, and 3 at this point, nor will it join the VLAN until and advertisement is received.
4. On Switch 3, port 4 receives advertisement of VIDs 1, 2, and 3 and becomes a member of VIDs 1, 2, and 3.
5. Port 5 advertises VIDs 1, 2,and 3, but port 5 is NOT a member of VIDs 1, 2, and 3 at this point.
6. Port 6 on the end device is statically configured to be a member of VID 3. Port 6 advertises VID 3.
7. Port 5 receives advertisement.
8. Port 4 advertises VID 3.
9. Port 3 receives advertisement of VID 3 AND becomes a member of VID 3. (Still not a member of VIDs 1 and 2 as it did not receive any advertisements for VID 1 or 2).
10. Port 1 advertises VID 3 of VID 3 AND becomes a member of VID 3. (Port 1 is still not a member of VIDs 1 and 2).

11. Port 2 receives advertisement of VID 3. (Port 2 was already statically configured for VIDs 1, 2, 3).

NOTE

If a static VLAN is configured on at least one port of a switch, and that port has established a link with another device, then all other ports of that switch will send advertisements for that VLAN.

In the following figure, tagged VLAN ports on switch "A" and switch "C" advertise VLANs 22 and 33 to ports on other GVRP-enabled switches that can dynamically join the VLANs. A port can learn of a dynamic VLAN through devices that are not aware of GVRP (Switch "B").

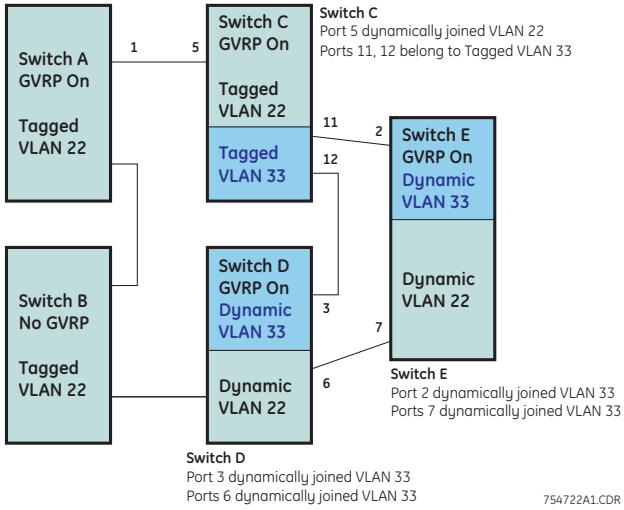


FIGURE 11–2: VLAN assignment in GVRP enabled switches

An "unknown VLAN" is a VLAN that the switch learns of by GVRP. For example, suppose that port 1 on switch "A" is connected to port 5 on switch "C". Because switch "A" has VLAN 22 statically configured, while switch "C" does not have this VLAN statically configured, VLAN 22 is handled as an "Unknown VLAN" on port 5 in switch "C". Conversely, if VLAN 22 was statically configured on switch C, but port 5 was not a member, port 5 would become a member when advertisements for VLAN 22 were received from switch "A". GVRP provides a per-port join-request option which can be configured.

VLANs must be disabled in GVRP-unaware devices to allow tagged packets to pass through. A GVRP-aware port receiving advertisements has these options:

- If there is no static VLAN with the advertised VID on the receiving port, then dynamically create a VLAN with the same VID as in the advertisement, and allow that VLAN's traffic
- If the switch already has a static VLAN with the same VID as in the advertisement, and the port is configured to learn for that VLAN, then the port will dynamically join the VLAN and allow that VLAN's traffic.
- Ignore the advertisement for that VID and drop all GVRP traffic with that VID
- Don't participate in that VLAN
- A port belonging to a tagged or untagged static VLAN has these configurable options:

- Send VLAN advertisements, and also receive advertisements for VLANs on other ports and dynamically join those VLANs
- Send VLAN advertisements, but ignore advertisements received from other ports
- Avoid GVRP participation by not sending advertisements and dropping any advertisements received from other devices

Table 11–1: Port settings for GVRP operations

Unknown VLAN mode	Operations
Learn	Enables the port to dynamically join any VLAN for which it receives and advertisement, and allows the port to forward the advertisement it receives.
Block	Prevents the port from dynamically joining a VLAN that is not statically configured on the switch. The port will still forward advertisements that were received by the switch on other ports. Block should typically be used on ports in insecure networks where there is exposure to attack - such as ports where intruders can connect.
Disable	Causes the port to ignore and drop all the advertisements it receives from any source.

The `show-vlan` command displays a switch's current GVRP configuration, including the unknown VLANs.

show-vlan

A port must be enabled and configured to learn for it to be assigned to the dynamic VLAN. To send advertisements, one or more tagged or untagged static VLANs must be configured on one (or more) switches with GVRP enabled. The ML2400 software allows a dynamic VLAN to be converted to a static VLAN with the `static` command.

static *vlan=<VID>*

The `show vlan type=tag` command will display VID in case the VID is not known.

Example 11-1 illustrates how to convert a dynamic VLAN into a static VLAN.

As the following table indicates, a port that has a tagged or untagged static VLAN has the option for both generating advertisements and dynamically joining other VLANs.

Table 11–2: GVRP options

Per-port "unknown VLAN" (GVRP) configuration	Per-port static VLAN options		
	Tagged or untagged	Auto	Forbid
Learn	Generate advertisements. Forward advertisements for other VLANs. Receive advertisements and dynamically join any advertised VLAN	Receive advertisements and dynamically join any advertised VLAN that has the same VID as the static VLAN	Do not allow the port to become a member of this VLAN
Block	Generate advertisements. Forward advertisements received from other ports to other VLANs. Do not dynamically join any advertised VLAN	Receive advertisements and dynamically join any advertised VLAN that has the same VID	Do not allow the VLAN on this port
Disable	Ignore GVRP and drop all GVRP advertisements	Ignore GVRP and drop all GVRP advertisements	Do not allow the VLAN on this port

Example 11-1: Converting a dynamic VLAN to a static VLAN

```
ML2400# gvrp
ML2400(gvrp)## show-vlan

================================================
  VLAN ID  |  NAME          |  VLAN     |  STATUS
================================================
     1     |  Default VLAN  |  Static   |  Active
     2     |  Blue          |  Static   |  Active
    10     |  dyn10         |  Dynamic  |  Active
ML2400(gvrp)## static vlan=10
ML2400(gvrp)## show-vlan

================================================
  VLAN ID  |  NAME          |  VLAN     |  STATUS
================================================
     1     |  Default VLAN  |  Static   |  Active
     2     |  Blue          |  Static   |  Active
    10     |  dyn10         |  Static   |  Active
```

The unknown VLAN parameters are configured on a per interface basis using the CLI. The tagged, untagged, Auto, and Forbid options are configured in the VLAN context. Since dynamic VLANs operate as tagged VLANs, and it is possible that a tagged port on one device may not communicate with an untagged port on another device, GE Multilin recommends that you use tagged VLANs for the static VLANs.

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN
- Reconfigure the port to Block or Disable
- Disable GVRP
- Reboot the switch

The time-to-live for dynamic VLANs is 10 seconds. That is, if a port has not received an advertisement for an existing dynamic VLAN during the last 10 seconds, the port removes itself from that dynamic VLAN.

11.2 Configuring GVRP through the Command Line Interface

11.2.1 Commands

The commands used for configuring GVRP are shown below.

The `gvrp` command enables or disables GVRP.

gvrp *<enable|disable>*

The `show gvrp` command displays whether GVRP is disabled, along with the current settings for the maximum number of VLANs and the current primary VLAN.

show gvrp

The `set-ports` command set the state of the port to learn, block or disable for GVRP. Note the default state is disable.

set-ports *port=<port|list|range> state=<learn|block|disable>*

The set-forbid command sets the forbid GVRP capability on the ports specified.

set-forbid *vlan=<tag vlanid>*
forbid=<port-number|list|range>

The show-forbid command displays the ports with GVRP forbid capabilities.

show-forbid

The following example illustrates how to configure GVRP using the commands shown in this section.

11.2.2 GVRP Operation Notes

A dynamic VLAN must be converted to a static VLAN before it can have an IP address.

After converting a dynamic VLAN to a static VLAN use the “save” command to save the changes made - on a reboot the changes can be lost without the save command.

Within the same broadcast domain, a dynamic VLAN can pass through a device that is not GVRP-aware. This is because a hub or a switch that is not GVRP-aware will flood the GVRP (multicast) advertisement packets out all ports.

GVRP assigns dynamic VLANs as tagged VLANs. To configure the VLAN as untagged, first convert the tagged VLAN to a static VLAN.

Rebooting a switch on which a dynamic VLAN deletes that VLAN. However, the dynamic VLAN re-appears after the reboot if GVRP is enabled and the switch again receives advertisements for that VLAN through a port configured to add dynamic VLANs.

By receiving advertisements from other devices running GVRP, the switch learns of static VLANs from those devices and dynamically (automatically) creates tagged VLANs on the links to the advertising devices. Similarly, the switch advertises its static VLANs to other GVRP-aware devices.

A GVRP-enabled switch does not advertise any GVRP-learned VLANs out of the port(s) on which it originally learned of those VLANs.

Example 11-2: Configuring GVRP

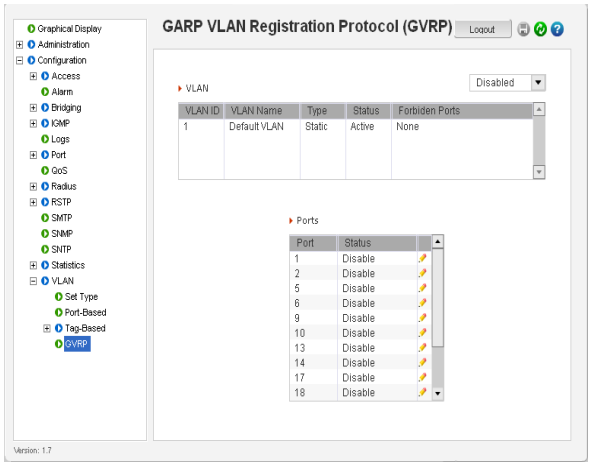
```
ML2400# gvrp
ML2400(gvrp)# show gvrp
  GVRP Status :  Enabled
ML2400(gvrp)## gvrp disable
  GVRP is now disabled
ML2400(gvrp)## gvrp enable
  GVRP enabled
ML2400(gvrp)## show-vlan
  ================================================
    VLAN ID  |  NAME          |  VLAN     |  STATUS
  ================================================
       1     |  Default VLAN  |  Static   |  Active
       2     |  Blue          |  Static   |  Active
      10     |  dyn10         |  Dynamic  |  Active
ML2400(gvrp)## static vlan=10
ML2400(gvrp)## show-vlan
  ================================================
    VLAN ID  |  NAME          |  VLAN     |  STATUS
  ================================================
       1     |  Default VLAN  |  Static   |  Active
       2     |  Blue          |  Static   |  Active
      10     |  dyn10         |  Static   |  Active
ML2400(gvrp)## set-forbid vlan=2 forbid=11-15
ML2400(gvrp)## show-forbid
  ==========================================
    VLAN ID  |  FORBIDDEN PORTS
  ==========================================
       1     |  None
       2     |  11, 12, 13, 14, 15
ML2400(gvrp)##
```

11.3 Configuring GVRP with EnerVista Secure Web Management Software

11.3.1 Example

To configure GVRP,

▷ Select the **Configuration > VLAN > GVRP** menu item.



From the GVRP menu screen, GVRP can be enabled or disabled using the drop down menu. Each specific port can be put in the Learn, Disable or Enable state as shown in Table 11–2: *GVRP options* on page 11–5.

The unknown VLAN parameters are configured on a per interface basis using the CLI. The tagged, untagged, Auto, and Forbid options are configured in the VLAN context. Since dynamic VLANs operate as tagged VLANs, and it is possible that a tagged port on one device may not communicate with an untagged port on another device, GE Multilin recommends that you use tagged VLANs for the static VLANs.

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN
- Reconfigure the port to Block or Disable
- Disable GVRP
- Save the configuration
- Reboot the switch

The time-to-live for dynamic VLANs is 10 seconds. That is, if a port has not received an advertisement for an existing dynamic VLAN during the last 10 seconds, the port removes itself from that dynamic VLAN.

Refer to *GVRP Operation Notes* on page 11–7 for additional information on using GVRP.

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 12: Spanning Tree Protocol (STP)

12.1 Overview

12.1.1 Description

The Spanning Tree Protocol was designed to avoid loops in an Ethernet network. An Ethernet network using switches can have redundant paths, which may cause loops. To prevent loops, the MultiLink Switch Software uses the spanning tree protocol (STP). Controlling the span in which traffic traverses is necessary as a manager of the software. It is also necessary to specify the parameters of STP. STP is available as the IEEE 802.1d protocol and is a standard of the IEEE.

12.1.2 Features and Operation

The switch uses the IEEE 802.1d Spanning Tree Protocol (STP). When STP is enabled, it ensures that only one path at a time is active between any two nodes on the network. In networks where more than one physical path exists between two nodes, STP ensures only a single path is active by blocking all redundant paths. Enabling STP is necessary to avoid loops and duplicate messages. This duplication leads to a “broadcast storm” or other erratic behavior that can bring down the network.

As recommended in the IEEE 802.1Q VLAN standard, the MultiLink family of switches uses single-instance STP. This means a single spanning tree is created to make sure there are no network loops associated with any of the connections to the switch. This works regardless of whether VLANs are configured on the switch. Thus, these switches do not distinguish between VLANs when identifying redundant physical links.

The switch automatically senses port identity and type, and automatically defines port cost and priority for each type. The software allows a manager to adjust the cost, priority, the mode for each port as well as the global STP parameter values for the switch.

While allowing only one active path through a network at any time, STP retains any redundant physical path to serve as a backup (blocked) path in case the existing active path fails. Thus, if an active path fails, STP automatically activates (unblocks) an available backup to serve as the new active path for as long as the original active path is down.

The table below lists the default values of the STP variables. Refer to the following section for detailed explanation on the variables. By default, STP is disabled. To use STP, it has to be manually enabled.

Table 12–1: STP default values

Variable or attribute	Default value
STP capabilities	Disabled
Reconfiguring general operation priority	32768
Bridge maximum age	20 seconds
Hello time	2 seconds
Forward delay	15 seconds
Reconfiguring per-port STP path cost	0
Priority	32768
Mode	Normal
Monitoring of STP	Not available
Root Port	Not set

12.2 Configuring STP

The `show stp` command lists the switch's full STP configuration, including general settings and port settings, regardless of whether STP is enabled or disabled (default).

show stp <*config*|*ports*>

Example 12-1 illustrates the `show stp` command with the `config` parameter.

The variables listed in this example are defined as follows

- **Spanning Tree Enabled (Global)**: Indicates whether STP is enabled or disabled globally; that is, if the values is YES, all ports have STP enabled. Otherwise, all ports have STP disabled.
- **Spanning Tree Enabled (Ports)**: Indicates which ports have STP enabled. In the example, ports 9 through 16 have STP enabled, but STP functionality is not enabled. As such, STP will not perform on these ports.
- **Bridge Priority**: Specifies the switch (bridge) priority value. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values indicate higher priority, and values range from 0 to 65535 with a default value of 32768.
- **Bridge Forward Delay**: Indicates the duration the switch waits from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds, with a default of 15.
- **Bridge Hello Time**: When the switch is the root device, this is the time between messages being transmitted. The value is from 1 to 10 seconds, with a default of 2.
- **Bridge Max Age**: This is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table. Value range from 6 to 40 seconds with default value of 20.
- **Root Port**: Indicates the port number elected as the root port of the switch. A root port of "0" indicates STP is disabled.
- **Root Path Cost**: A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost indicates more loops, a lower cost indicates fewer loops. More loops equal more traffic and a tree which requires a long time to converge - resulting in a slower system.
- **Designated Root**: Displays the MAC address of the bridge in the network elected or designated as the root bridge. When STP is not enabled, the switch designates itself as the root switch.
- **Designated Root Priority**: Shows the designated root bridge's priority. The default value is 32768.
- **Root Bridge Forward Delay**: Indicates the designated root bridge forward delay. This is the time the switch waits before switching from the listening to the

forwarding state. The default is 15 seconds, with a range of 4 to 30 seconds.

- **Root Bridge Hello Time**: Indicates the designated root bridge's hello time. Hello information is transmitted every 2 seconds.
- **Root Bridge Max Age**: Indicates the designated root bridge maximum age, after which it discards the information as being old and receives new updates.

These variables can be changed using the "priority", "cost", "port" and "timers" commands described later in this chapter.

Example 12-2 illustrates the `show stp` command with the `ports` parameter. The variables listed in this example are defined as follows:

- ***Port#***: indicates the port number. Value ranges from 01 to max number of ports in the switch
- ***Type***: indicates the type of port - TP indicates Twisted Pair

Example 12-1: Viewing STP configuration

```
ML2400# show stp config
  STP CONFIGURATION
  -----------------
  Spanning Tree Enabled(Global) : NO
  Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
  Protocol                      : Normal STP
  Bridge ID                     : 80:00:00:20:06:25:ed:80
  Bridge Priority               : 32768
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 2
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:80
  Designated Root Priority      : 32768
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 2
  Root Bridge Max Age           : 20

  RSTP CONFIGURATION
  -----------------
  Rapid STP/STP Enabled(Global) : NO
ML2400#
```

Example 12-2: Viewing STP ports

```
ML2400# show stp ports
  STP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type         Priority  Path Cost  State       Des. Bridge              Des. Port
  ------------------------------------------------------------------------------------
  09     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:09
  10     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
  11     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
  12     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
  13     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0d
  14     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
  15     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
  16     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
ML2400#
```

- ***Priority***: STP uses this to determine which ports are used for forwarding. Lower the number means higher priority. Value ranges from 0 to 255. Default is 128
- ***Path Cost***: This is the assigned port cost value used for the switch to determine the forwarding points. Values range from 1 to 65535
- ***State***: indicates the STP state of individual ports. Values can be Listening, Learning, Forwarding, Blocking and Disabled.
- ***Des. Bridge***: This is the port's designated root bridge
- ***Des. Port***: This is the port's designated root port

To enable or disable STP, enter the STP configuration mode via the `stp` command and use the `stp enable` or `stp disable` command.

To `stp` command enters STP configuration mode:

stp

The `enable` and `disable` parameters start (enable) or stop (disable) STP.

stp *<enable|disable>*

The `stp` and `rstp` parameters set the spanning tree protocol to be IEEE 802.1d or 802.1w (Rapid Spanning Tree Protocol).

set stp *type=<stp|rstp>*

The `show active-stp` command display which version of STP is currently active.

show active-stp

Incorrect STP settings can adversely affect network performance. GE recommends starting with the default STP settings. Changing the settings requires a detailed understanding of STP. For more information on STP, please refer to the IEEE 802.1d standard.

It is always a good idea to check which mode of STP is active. If the proper mode is not active, the configuration command `stp` will not be understood. To set the proper mode, use the `set stp` command.

Example 12-3 shows how to enable STP using the above commands.

The `priority` command specifies the port or switch level priority. When a port(s) are specified the priority is associated with ports and their value is 0 to 255. If no ports are specified, then the switch (bridge) priority is specified and its value is 0 to 65535. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values mean higher priority. The default value is 32768.

Example 12-3: Enabling STP

```
ML2400# show active-stp

  Current Active Mode: RSTP.
  RSTP is Disabled.

ML2400# stp

  ERROR: Invalid Command

ML2400# set stp type=stp

  STP Mode set to STP.

ML2400# stp

ML2400(stp)## stp enable

  Successfully set the STP status

ML2400(stp)## show stp config

  STP CONFIGURATION
  -----------------
  Spanning Tree Enabled(Global) : YES
  Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
  Protocol                      : Normal STP
  Bridge ID                     : 80:00:00:20:06:25:ed:80
  Bridge Priority               : 32768
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 2
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:80
  Designated Root Priority      : 32768
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 2
  Root Bridge Max Age           : 20

  RSTP CONFIGURATION
  -----------------
  Rapid STP/STP Enabled(Global) : NO

ML2400(stp)## show stp ports

  STP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type         Priority  Path Cost  State       Des. Bridge              Des. Port
  ------------------------------------------------------------------------------------
  09     TP(10/100)   128       100        Forwarding  80:00:00:20:06:25:ed:80  80:09
  10     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
  11     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
  12     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
  13     TP(10/100)   128       19         Forwarding  80:00:00:20:06:25:ed:80  80:0d
  14     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
  15     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
  16     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:10

ML2400(stp)##
```

priority *[port=<number|list|range>]*
value=<0-255 | 0-65535>

The `cost` command is port specific. A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means the link is "more expensive" to use and falls in the passive mode compared to the link with a lower cost. Value ranges from 0 to 65535, with a default value of 32768.

cost *port=<number|list|range>*
value=<0-65535>

The `port` command assigns ports to STP. If you are unsure, let the software make the decisions. The `status` parameter enables or disables a port from participating in STP discovery. Its best to only allow trunk ports to participate in STP. End stations need not participate in STP process.

port *port=<number|list|range>*
status=<enable|disable>

The `timers` command changes the STP forward delay, hello timer and aging timer values. The `forward-delay` parameter indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds with a default value of 15. When the switch is the root device, the `hello` parameter represents the time between messages being transmitted. The value is from 1 to 10 seconds with a default value is 2. The `age` parameter is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table again. Value ranges from 6 to 40 seconds with default value of 20.

timers *forward-delay=<4-30> hello=<1-10> age=<6-40>*

Example 12-4: Configuring STP parameters

```
ML2400(stp)## show stp config

  STP CONFIGURATION
  -----------------
  Spanning Tree Enabled(Global) : NO
  Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
  Protocol                      : Normal STP
  Bridge ID                     : 80:00:00:20:06:25:ed:80
  Bridge Priority               : 32768
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 2
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:80
  Designated Root Priority      : 32768
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 2
  Root Bridge Max Age           : 20

  RSTP CONFIGURATION
  -----------------
  Rapid STP/STP Enabled(Global) : NO

ML2400(stp)## show stp ports

  STP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type        Priority  Path Cost  State       Des. Bridge              Des. Port
  ------------------------------------------------------------------------------------
  09     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:09
  10     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
  11     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
  12     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
  13     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0d
  14     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
  15     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
  16     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:10

ML2400(stp)## stp enable

  Successfully set the STP status
```

(continued on next page)

Configuring STP parameters (continued)

ML2400(stp)## show stp config

```
STP CONFIGURATION
-----------------
Spanning Tree Enabled(Global) : YES
Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
Protocol                      : Normal STP
Bridge ID                     : 80:00:00:20:06:25:ed:80
Bridge Priority               : 32768
Bridge Forward Delay          : 15
Bridge Hello Time             : 2
Bridge Max Age                : 20
Root Port                     : 0
Root Path Cost                : 0
Designated Root               : 80:00:00:20:06:25:ed:80
Designated Root Priority      : 32768
Root Bridge Forward Delay     : 15
Root Bridge Hello Time        : 2
Root Bridge Max Age           : 20

RSTP CONFIGURATION
-----------------
Rapid STP/STP Enabled(Global) : NO
```

Ports that have connected devices now participate in STP.

ML2400(stp)## show stp ports

```
STP Port Configuration

-------------------------------------------------------------------------------
Port#  Type        Priority  Path Cost  State       Des. Bridge              Des. Port
-------------------------------------------------------------------------------
09     TP(10/100)  128       100        Forwarding  80:00:00:20:06:25:ed:80  80:09
10     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
11     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
12     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
13     TP(10/100)  128       19         Forwarding  80:00:00:20:06:25:ed:80  80:0d
14     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
15     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
16     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
```

ML2400(stp)## priority value=15535

```
Successfully set the bridge priority
```

STP is now enabled. Note the default values for the discussed variables.

ML2400(stp)## show stp config

```
STP CONFIGURATION
-----------------
Spanning Tree Enabled(Global) : YES
Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
Protocol                      : Normal STP
Bridge ID                     : 80:00:00:20:06:25:ed:80
Bridge Priority               : 15535
Bridge Forward Delay          : 15
Bridge Hello Time             : 2
Bridge Max Age                : 20
Root Port                     : 0
Root Path Cost                : 0
Designated Root               : 80:00:00:20:06:25:ed:80
Designated Root Priority      : 15535
Root Bridge Forward Delay     : 15
Root Bridge Hello Time        : 2
Root Bridge Max Age           : 20
```

(continued on next page)

Configuring STP parameters (continued)

```
RSTP CONFIGURATION
-----------------
Rapid STP/STP Enabled(Global) : NO
```

ML2400(stp)## priority port=13 value=20

```
Successfully set the priority for port 13
```

ML2400(stp)## show stp ports

```
STP Port Configuration

-------------------------------------------------------------------------------
Port#  Type         Priority  Path Cost  State       Des. Bridge              Des. Port
-------------------------------------------------------------------------------
09     TP(10/100)   128       100        Forwarding  80:00:00:20:06:25:ed:80  80:09
10     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
11     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
12     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
13     TP(10/100)   20        19         Forwarding  80:00:00:20:06:25:ed:80  80:0d
14     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
15     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
16     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
```

ML2400(stp)## cost port=13 value=20

```
Setting cost for STP...Successfully set the path cost for port 13
```

ML2400(stp)## show stp ports

```
STP Port Configuration

-------------------------------------------------------------------------------
Port#  Type         Priority  Path Cost  State       Des. Bridge              Des. Port
-------------------------------------------------------------------------------
09     TP(10/100)   128       100        Forwarding  80:00:00:20:06:25:ed:80  80:09
10     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
11     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
12     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
13     TP(10/100)   20        20         Forwarding  80:00:00:20:06:25:ed:80  80:0d
14     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
15     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
16     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
```

ML2400(stp)## port port=9 status=disable

```
Successfully set the STP status for port 9
```

ML2400(stp)## show stp ports

Since port 9 does not participate in STP, it is not listed here. Any changes made to STP parameters on port 9 will be ignored

```
STP Port Configuration

-------------------------------------------------------------------------------
Port#  Type         Priority  Path Cost  State       Des. Bridge              Des. Port
-------------------------------------------------------------------------------
10     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
11     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
12     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
13     TP(10/100)   20        20         Forwarding  80:00:00:20:06:25:ed:80  80:0d
14     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
15     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
16     TP(10/100)   128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
```

(continued on next page)

Configuring STP parameters (continued)

```
ML2400 (stp) ## port port=9 status=enable
  Successfully set the STP status for port 9
ML2400(stp)## show stp ports
  STP Port Configuration

  ----------------------------------------------------------------------------------------
  Port#  Type         Priority  Path Cost  State       Des. Bridge              Des. Port
  ----------------------------------------------------------------------------------------
  09     TP(10/100)  128       100        Forwarding  80:00:00:20:06:25:ed:80  80:09
  10     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0a
  11     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0b
  12     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0c
  13     TP(10/100)  20        20         Forwarding  80:00:00:20:06:25:ed:80  80:0d
  14     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0e
  15     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:0f
  16     TP(10/100)  128       100        Disabled    80:00:00:20:06:25:ed:80  80:10
ML2400(stp)## show stp config
  STP CONFIGURATION
  -----------------
  Spanning Tree Enabled(Global) : YES
  Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
  Protocol                      : Normal STP
  Bridge ID                     : 80:00:00:20:06:25:ed:80
  Bridge Priority               : 15535
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 2
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:80
  Designated Root Priority      : 15535
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 2
  Root Bridge Max Age           : 20

  RSTP CONFIGURATION
  -----------------
  Rapid STP/STP Enabled(Global) : NO
```

The age parameter is out of range as per the IEEE 802.1d specifications.

```
ML2400(stp)## timers forward-delay=20 hello=5 age=40
  ERROR:  Invalid Values
          Max Age <= (2*(Forward-Delay-1)) and Max Age >= (2*(Hello-Time+1))
ML2400(stp)## timers forward-delay=20 hello=5 age=30
  Successfully set the bridge time parameters
```

(continued on next page)

Configuring STP parameters (continued)

```
ML2400(stp)## show stp config

  STP CONFIGURATION
  -----------------
  Spanning Tree Enabled(Global) : YES
  Spanning Tree Enabled(Ports)  : YES, 9,10,11,12,13,14,15,16
  Protocol                      : Normal STP
  Bridge ID                     : 80:00:00:20:06:25:ed:80
  Bridge Priority               : 15535
  Bridge Forward Delay          : 20
  Bridge Hello Time             : 5
  Bridge Max Age                : 30
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:80
  Designated Root Priority      : 15535
  Root Bridge Forward Delay     : 20
  Root Bridge Hello Time        : 5
  Root Bridge Max Age           : 30

  RSTP CONFIGURATION
  -----------------
  Rapid STP/STP Enabled(Global) : NO

ML2400(stp)##
```

Multilink ML2400

Ethernet Communications Switch

Chapter 13: Rapid Spanning Tree Protocol

13.1 Overview

13.1.1 Description

The Rapid Spanning Tree Protocol (RTSP), like STP, was designed to avoid loops in an Ethernet network. Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w) is an evolution of the Spanning Tree Protocol (STP) (802.1d standard) and provides for faster spanning tree convergence after a topology change.

13.1.2 RSTP Concepts

The IEEE 802.1d Spanning Tree Protocol (STP) was developed to allow the construction of robust networks that incorporate redundancy while pruning the active topology of the network to prevent loops. While STP is effective, it requires that frame transfer must halt after a link outage until all bridges in the network are sure to be aware of the new topology. Using STP (IEEE 802.1d) recommended values, this period lasts 30 seconds.

The Rapid Spanning Tree Protocol (IEEE 802.1w) is a further evolution of the 802.1d Spanning Tree Protocol. It replaces the settling period with an active handshake between switches (bridges) that guarantees topology information to be rapidly propagated through the network. RSTP converges in less than one second. RSTP also offers a number of other significant innovations. These include

- Topology changes in STP must be passed to the root bridge before they can be propagated to the network. Topology changes in RSTP can be originated from and acted upon by any designated switch (bridge), leading to more rapid propagation of address information
- STP recognizes one state - blocking for ports that should not forward any data or information. RSTP explicitly recognizes two states or blocking roles - alternate and backup port including them in computations of when to learn and forward and when to block

- STP relays configuration messages received on the root port going out of its designated ports. If an STP switch (bridge) fails to receive a message from its neighbor it cannot be sure where along the path to the root a failure occurred. RSTP switches (bridges) generate their own configuration messages, even if they fail to receive one from the root bridge. This leads to quicker failure detection
- RSTP offers edge port recognition, allowing ports at the edge of the network to forward frames immediately after activation while at the same time protecting them against loops
- An improvement in RSTP allows configuration messages to age more quickly preventing them from "going around in circles" in the event of a loop

RSTP has three states. They are discarding, learning and forwarding.

The ***discarding*** state is entered when the port is first taken into service. The port does not learn addresses in this state and does not participate in frame transfer. The port looks for STP traffic in order to determine its role in the network. When it is determined that the port will play an active part in the network, the state will change to ***learning***. The learning state is entered when the port is preparing to play an active member of the network. The port learns addresses in this state but does not participate in frame transfer. In a network of RSTP switches (bridges) the time spent in this state is usually quite short. RSTP switches (bridges) operating in STP compatibility mode will spend between 6 to 40 seconds in this state. After 'learning' the bridge will place the port in the ***forwarding*** state. While in this state the port both learns addresses and participates in frame transfer while in this state.

The result of these enhanced states is that the IEEE 802.1d version of spanning tree (STP) can take a fairly long time to resolve all the possible paths and to select the most efficient path through the network. The IEEE 802.1w Rapid reconfiguration of Spanning Tree significantly reduces the amount of time it takes to establish the network path. The result is reduced network downtime and improved network robustness. In addition to faster network reconfiguration, RSTP also implements greater ranges for port path costs to accommodate the higher connection speeds that are being implemented.

Proper implementations of RSTP (by switch vendors) is designed to be compatible with IEEE 802.1d STP. GE recommends that you employ RSTP or STP in your network.

13.1.3 Transition from STP to RSTP

IEEE 802.1w RSTP is designed to be compatible with IEEE 802.1D STP. Even if all the other devices in your network are using STP, you can enable RSTP on the MultiLink family of switches. The default configuration values of the RSTP available in ML2400 software will ensure that your switch will inter-operate effectively with the existing STP devices. RSTP automatically detects when the switch ports are connected to non-RSTP devices using spanning tree and communicates with those devices using 802.1d STP BPDU packets.

Even though RSTP inter-operates with STP, RSTP is more efficient at establishing the network path and network convergence in case of a very fast failure. As such, GE recommends that all network devices be updated to support RSTP. RSTP offers convergence times typically less than one second. However, to make best use of RSTP and achieve the fastest possible convergence times, there are some changes required to the RSTP default configuration.

1. Under some circumstances, it is possible for the rapid state transitions employed by RSTP to result in an increase in the rates of frame duplication and the order in which the frames are sent and received. To allow RSTP switches to support applications and protocols that may be sensitive to frame duplication and out of sequence frames, RSTP may have to be explicitly set to be compatible with STP. This requires setting the "Force Protocol Version" parameter to be STP compatible. This parameter should be set to all ports on a given switch.
2. As indicated above, one of the benefits of RSTP is the implementation of a larger range of port path costs that accommodates higher network speeds. New default values have been implemented for path costs associated with the different network speeds. This may create incompatibility between devices running the older implementations of STP a switch running RSTP.
3. At any given time, the software can support either STP or RSTP but not both.

13.2 Configuring RSTP through the Command Line Interface

13.2.1 Normal RSTP

The commands to setup and configure RSTP are as follows. The `set stp` command sets the switch to support RSTP or STP. It is necessary to save and reboot the switch after this command.

set stp *type=<stp|rstp>* -

The `rstp` command enters the RSTP configuration mode and enables/disabled RSTP. By default, RSTP is disabled and has to be manually activated.

rstp
rstp *<enable|disable>*
rstp *<romode|normal>*

The syntax for the `port` command on RSTP is shown below.

port *port=<number|list|range> [status=<enable|disable>] [migration=<enable>] [edge=<enable|disable>] [p2p=<on|off|auto>]*

The `p2p` parameter sets the "point-to-point" value to off on all ports connected to shared LAN segments (i.e. connections to hubs). The default value is `auto`. P2P ports would typically be end stations or computers on the network.

The `edge` parameter enables/disables all ports connected to other hubs, bridges and switches as edge ports.

The `migration` parameter is set for all ports connected to devices such as hubs, bridges and switches known to support IEEE 802.1d STP services but not RSTP services

The `show active-stp` command displays whether STP or RSTP is running.

show active-stp

The `show stp` command display the RSTP or STP parameters.

show stp *<config|ports>*

Users may notice extended recovery time if there is a mix of firmware revisions in the Mesh or Ring.

The variables listed by the `show stp config` command are:

- **Rapid Spanning Tree Enabled (Global)**: Indicates whether STP is enabled or disabled globally i.e. if the values is YES, all ports have STP enabled, otherwise, all ports have STP disabled.
- **Rapid Spanning Tree Enabled Ports**: Indicates which ports have RSTP enabled.
- **Protocol**: Indicates whether STP or RSTP is being used. It also indicates if RSTP is used in Smart RSTP (ring-only mode) or normal mode.
- **Bridge Priority**: Specifies the switch (bridge) priority value. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values mean higher priority. Values range from 0 to 65535 with a default of 0.
- **Bridge Forward Delay**: Indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds with a default of 15.
- **Bridge Hello Time**: When the switch is the root device, this is the time between messages being transmitted. The value is from 1 to 10 seconds with a default of 2.
- **Bridge Max Age**: This is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table again. Values range from 6 to 40 seconds with a default value of 20.
- **Root Port**: Indicates the port number, which is elected as the root port of the switch. A root port of "0" indicates STP is disabled.
- **Root Path Cost**: A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means more loops; a lower cost means fewer loops. More loops equal more traffic and a tree which takes a long time to converge, resulting in a slower system.
- **Designated Root**: Shows the MAC address of the bridge in the network elected or designated as the root bridge.
- **Designated Root Priority**: Shows the designated root bridge's priority. The default value is 0.
- **Root Bridge Forward Delay**: Indicates the designated root bridge's forward delay. This is the time the switch waits before it switches from the listening to the forwarding state. This value can be set between 4 to 30 seconds, with a default of 15.
- **Root Bridge Hello Time**: Indicates the designated root bridge's hello time. Hello information is sent out every 2 seconds.
- **Root Bridge Max Age**: Indicates the designated root bridge's maximum age, after which it discards the information as being old and receives new updates.
- **Topology Change Count**: Since the last reboot, the number of times the topology has changed. Use this in conjunction with "show uptime" to find the frequency of the topology changes.
- **Time Since topology Change**: The number of seconds since the last topology change.

Example 13-1: Enabling RSTP and reviewing the RSTP variables

```
ML2400# rstp
ML2400(rstp)## show stp config

  RSTP CONFIGURATION
  -----------------
  Rapid STP/STP Enabled(Global) : NO
ML2400(rstp)## rstp enable

  Successfully set the RSTP status
ML2400(rstp)## show active-stp

  Current Active Mode: RSTP.
  RSTP is Enabled.
ML2400(rstp)## show stp config

  RSTP CONFIGURATION
  -----------------
  Rapid STP/STP Enabled(Global) : YES
  RSTP/STP Enabled Ports        : 9,10,11,12,13,14,15,16
  Protocol                      : Normal RSTP
  Bridge ID                     : 80:00:00:20:06:25:ed:89
  Bridge Priority               : 0
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 2
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:89
  Designated Root Priority      : 0
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 2
  Root Bridge Max Age           : 20
  Topology Change Count         : 0
  Time Since Topology Chg       : 12
ML2400(rstp)## show stp config

  RSTP CONFIGURATION
  -----------------
  Rapid STP/STP Enabled(Global) : YES
  RSTP/STP Enabled Ports        : 9,10,11,12,13,14,15,16
  Protocol                      : Normal RSTP Ring Only Mode
  Bridge ID                     : 80:00:00:20:06:25:ed:89
  Bridge Priority               : 0
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 2
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:89
  Designated Root Priority      : 0
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 2
  Root Bridge Max Age           : 20
  Topology Change Count         : 0
  Time Since Topology Chg       : 12
```

The variables listed by the `show stp ports` command are:

- **Port#**: Indicates the port number. The value ranges from 1 to the maximum number of ports in the switch.
- **Type**: Indicates the type of port. TP indicates twisted pair.
- **Priority**: STP uses this to determine which ports are used for forwarding. Lower numbers indicate higher priority. The values range from 0 to 255, with a default of 128.
- **Path Cost**: This is the assigned port cost value used for the switch to determine the forwarding points. Values range from 1 to 2000000. Lower values indicate a lower cost and hence the preferred route. The costs for different Ethernet speeds are indicated below. The Path cost in STP is compared to the path cost in RSTP.

Table 13–1: Path cost as defined in IEEE 802.1d / 802.1w

Port type	STP path cost	RSTP path cost
10 Mbps	100	2000000
100 Mbps	19	200000
1 Gbps	4	20000
10 Gbps	2	2000

- **State**: Indicates the STP state of individual ports. Values can be Listening, Learning, Forwarding, Blocking and Disabled.
- **Des. Bridge**: This is the port's designated root bridge
- **Des. Port**: This is the port's designated root port

Example 13-2: Reviewing the RSTP port parameters

```
ML2400(rstp)## show stp ports

  RSTP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type         Priority  Path Cost  State       Des. Bridge               Des. Port
  ------------------------------------------------------------------------------------
  09     TP(10/100)   128       2000000    Forwarding  80:00:00:20:06:25:ed:89   80:09
  10     TP(10/100)   128       2000000    Disabled                              80:0a
  11     TP(10/100)   128       2000000    Disabled                              80:0b
  12     TP(10/100)   128       2000000    Disabled                              80:0c
  13     TP(10/100)   20        200000     Forwarding  80:00:00:20:06:25:ed:89   80:0d
  14     TP(10/100)   128       2000000    Disabled                              80:0e
  15     TP(10/100)   128       2000000    Disabled                              80:0f
  16     TP(10/100)   128       2000000    Disabled                              80:10
ML2400(rstp)##
```

Another example of the same command, from a larger network with several switches is shown in Example 13-3. Note the `show stp ports` command can be executed from the manager level prompt or from RSTP configuration state as shown in the screen captures earlier.

Example 13-3: RSTP information from a network with multiple switches

```
ML2400(rstp)## show stp ports

  RSTP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type         Priority  Path Cost  State       Des. Bridge              Des. Port
  ------------------------------------------------------------------------------------
  01     TP(10/100)   128       2000000    Disabled                             00:01
  02     TP(10/100)   128       2000000    Disabled                             00:02
  03     TP(10/100)   128       2000000    Disabled                             00:03
  04     TP(10/100)   128       2000000    Disabled                             00:04
  05     TP(10/100)   20        2000000    Disabled                             00:05
  06     TP(10/100)   128       200000     Forwarding  80:00:00:20:06:30:00:01  00:06
  07     TP(10/100)   128       200000     Disacrding  80:00:00:20:06:2b:0f:e1  00:07
  08     TP(10/100)   128       2000000    Disabled                             00:08
  09     Gigabit      128       20000      Forwarding  80:00:00:20:06:2b:0f:e1  00:09
  10     Gigabit      128       20000      Forwarding  80:00:00:20:06:30:00:01  00:0a
ML2400(rstp)##
```

In this example, ports 9 and 10 have a path cost of 20000 and are the least cost paths. These ports are connected to other switches and the ports are enabled as forwarding ports. Ports 6 and 7 are also connected to other switches. From the state column, it indicates that port 7 is in a standby state as that port is discarding all traffic.

More CLI commands associated with RSTP in the RSTP configuration mode are shown below. The `forceversion` command sets the STP or RSTP compatibility mode.

forceversion *<stp|rstp>*

The `show-forceversion` command displays the current forced version.

show-forceversion

The `show-timers` command displays the values of the timers set for RSTP.

show-timers

The `priority` command specifies the switch (bridge) priority value. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values mean higher priority. The value ranges from 0 to 65535 with a default of 32768. When port are specified, the priority is associated with ports and their value is 0 to 255.

priority *[port=<number|list|range>]*
value=<0-255|0-65535>

A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means the link is "more expensive" to use and falls in the passive mode compared to the link with a lower cost. The value of the `cost` command ranges from 0 to 65535, with a default of 32768.

cost *port=<number|list|range>*
value=<0-65535>

The `port` command assigns ports for RSTP. Note that specific ports may not need to participate in RSTP process. These ports typically would be end-stations. If unsure, it is best to let the software make the decisions.

port *port=<number|list|range> status=<enable|disable>*

The `status` parameter enables or disables a port from participating in RSTP discovery. Its best to only allow trunk ports to participate in RSTP; end stations need not participate in the RSTP process.

The `timers` command changes the STP forward delay, hello timer and aging timer values.

timers *forward-delay=<4-30> hello=<1-10> age=<6-40>*

The `forward-delay` parameter indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds with a default of 15.

The `hello` parameter represents the time between messages being transmitted when the switch is the root device. The value is 1 to 10 seconds, with a default of 2.

The `age` parameter is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table again. Value ranges from 6 to 40 seconds with default value of 20.

Example 13-4: Configuring RSTP

```
ML2400# rstp
ML2400(rstp)## show stp config

  RSTP CONFIGURATION
  ------------------
  Rapid STP/STP Enabled(Global) : NO
ML2400(rstp)## show active-stp

  Current Active Mode: RSTP.
  RSTP is Disabled.
ML2400(rstp)## rstp enable

  Successfully set the RSTP status
ML2400(rstp)## show active-stp

  Current Active Mode: RSTP.
  RSTP is Enabled.
ML2400(rstp)## show stp config

  RSTP CONFIGURATION
  ------------------
  Rapid STP/STP Enabled(Global) : YES
  RSTP/STP Enabled Ports        : 9,10,11,12,13,14,15,16
  Protocol                      : Normal RSTP
  Bridge ID                     : 80:00:00:20:06:25:ed:89
  Bridge Priority               : 0
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 02
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:89
  Designated Root Priority      : 0
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 02
  Root Bridge Max Age           : 20
  Topology Change Count         : 0
  Time Since Topology Chg       : 33
ML2400(rstp)## show stp ports

  RSTP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type         Priority  Path Cost  State       Des. Bridge              Des. Port
  ------------------------------------------------------------------------------------
  09     TP(10/100)   128       2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
  10     TP(10/100)   128       2000000    Disabled                             00:0a
  11     TP(10/100)   128       2000000    Disabled                             00:0b
  12     TP(10/100)   128       2000000    Disabled                             00:0c
  13     TP(10/100)   128       200000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
  14     TP(10/100)   128       2000000    Disabled                             00:0e
  15     TP(10/100)   128       2000000    Disabled                             00:0f
  16     TP(10/100)   128       2000000    Disabled                             00:10
ML2400(rstp)## forceversion rstp

  Error: Force Version already set to Normal RSTP
```

Check the status of STP or RSTP. These commands show if STP or RSTP is enabled.

(continued on next page)

Configuring RSTP (continued)

```
ML2400(rstp)## forceversion stp
ML2400(rstp)## show-forceversion

  Force Version : Force to STP only
ML2400(rstp)## show stp config

  RSTP CONFIGURATION
  ------------------
  Rapid STP/STP Enabled(Global) : YES
  RSTP/STP Enabled Ports        : 9,10,11,12,13,14,15,16
  Protocol                      : Force to STP only
  Bridge ID                     : 80:00:00:20:06:25:ed:89
  Bridge Priority               : 0
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 02
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:89
  Designated Root Priority      : 0
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 02
  Root Bridge Max Age           : 20
  Topology Change Count         : 0
  Time Since Topology Chg       : 100
ML2400(rstp)## forceversion rstp
ML2400(rstp)## show-forceversion

  Force Version : Normal RSTP
ML2400(rstp)## show stp config

  RSTP CONFIGURATION
  ------------------
  Rapid STP/STP Enabled(Global) : YES
  RSTP/STP Enabled Ports        : 9,10,11,12,13,14,15,16
  Protocol                      : Normal RSTP
  Bridge ID                     : 80:00:00:20:06:25:ed:89
  Bridge Priority               : 0
  Bridge Forward Delay          : 15
  Bridge Hello Time             : 02
  Bridge Max Age                : 20
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:89
  Designated Root Priority      : 0
  Root Bridge Forward Delay     : 15
  Root Bridge Hello Time        : 02
  Root Bridge Max Age           : 20
  Topology Change Count         : 0
  Time Since Topology Chg       : 141
ML2400(rstp)## show-timers

  Forward Delay Timer : 15 sec
  Hello Timer         : 2 sec
  Max Age             : 20 sec
```

The `forceversion` capability can be used for compatibility with STP devices. In this example, the switch is forced to STP mode.

Using `forceversion`, the switch is now operating using RSTP. Note the `show stp config` command also indicates the switch protocol is RSTP.

(continued on next page)

Configuring RSTP (continued)

```
ML2400(rstp)## show stp ports
  RSTP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type        Priority  Path Cost  State       Des. Bridge              Des. Port
  ------------------------------------------------------------------------------------
  09     TP(10/100)  128       2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
  10     TP(10/100)  128       2000000    Disabled                             00:0a
  11     TP(10/100)  128       2000000    Disabled                             00:0b
  12     TP(10/100)  128       2000000    Disabled                             00:0c
  13     TP(10/100)  128       200000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
  14     TP(10/100)  128       2000000    Disabled                             00:0e
  15     TP(10/100)  128       2000000    Disabled                             00:0f
  16     TP(10/100)  128       2000000    Disabled                             00:10
ML2400(rstp)## priority port=13 value=100
ML2400(rstp)## show stp ports
  RSTP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type        Priority  Path Cost  State       Des. Bridge              Des. Port
  ------------------------------------------------------------------------------------
  09     TP(10/100)  128       2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
  10     TP(10/100)  128       2000000    Disabled                             00:0a
  11     TP(10/100)  128       2000000    Disabled                             00:0b
  12     TP(10/100)  128       2000000    Disabled                             00:0c
  13     TP(10/100)  100       200000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
  14     TP(10/100)  128       2000000    Disabled                             00:0e
  15     TP(10/100)  128       2000000    Disabled                             00:0f
  16     TP(10/100)  128       2000000    Disabled                             00:10
ML2400(rstp)## cost port=13 value=250000
ML2400(rstp)## show stp ports
  RSTP Port Configuration

  ------------------------------------------------------------------------------------
  Port#  Type        Priority  Path Cost  State       Des. Bridge              Des. Port
  ------------------------------------------------------------------------------------
  09     TP(10/100)  128       2000000    Forwarding  80:00:00:20:06:25:ed:89  00:09
  10     TP(10/100)  128       2000000    Disabled                             00:0a
  11     TP(10/100)  128       2000000    Disabled                             00:0b
  12     TP(10/100)  128       2000000    Disabled                             00:0c
  13     TP(10/100)  100       250000     Forwarding  80:00:00:20:06:25:ed:89  00:0d
  14     TP(10/100)  128       2000000    Disabled                             00:0e
  15     TP(10/100)  128       2000000    Disabled                             00:0f
  16     TP(10/100)  128       2000000    Disabled                             00:10
ML2400(rstp)## port port=9 status=disable
```

(continued on next page)

Configuring RSTP (continued)

```
ML2400(rstp)## show stp ports
  RSTP Port Configuration

  ------------------------------------------------------------------------------
  Port#  Type        Priority  Path Cost  State       Des. Bridge               Des. Port
  ------------------------------------------------------------------------------
  09     TP(10/100)  128       2000000    No STP                                00:09
  10     TP(10/100)  128       2000000    Disabled                              00:0a
  11     TP(10/100)  128       2000000    Disabled                              00:0b
  12     TP(10/100)  128       2000000    Disabled                              00:0c
  13     TP(10/100)  100       250000     Forwarding  80:00:00:20:06:25:ed:89   00:0d
  14     TP(10/100)  128       2000000    Disabled                              00:0e
  15     TP(10/100)  128       2000000    Disabled                              00:0f
  16     TP(10/100)  128       2000000    Disabled                              00:10
ML2400(rstp)## port port=9 status=enable
ML2400(rstp)## show stp ports
  RSTP Port Configuration

  ------------------------------------------------------------------------------
  Port#  Type        Priority  Path Cost  State       Des. Bridge               Des. Port
  ------------------------------------------------------------------------------
  09     TP(10/100)  128       2000000    Forwarding  80:00:00:20:06:25:ed:89   00:09
  10     TP(10/100)  128       2000000    Disabled                              00:0a
  11     TP(10/100)  128       2000000    Disabled                              00:0b
  12     TP(10/100)  128       2000000    Disabled                              00:0c
  13     TP(10/100)  100       250000     Forwarding  80:00:00:20:06:25:ed:89   00:0d
  14     TP(10/100)  128       2000000    Disabled                              00:0e
  15     TP(10/100)  128       2000000    Disabled                              00:0f
  16     TP(10/100)  128       2000000    Disabled                              00:10
ML2400(rstp)## timers forward-delay=20 hello=5 age=30
  Successfully set the bridge time parameters
ML2400(rstp)## show stp config
  RSTP CONFIGURATION
  ------------------
  Rapid STP/STP Enabled(Global) : YES
  RSTP/STP Enabled Ports        : 9,10,11,12,13,14,15,16
  Protocol                      : Normal RSTP
  Bridge ID                     : 80:00:00:20:06:25:ed:89
  Bridge Priority               : 0
  Bridge Forward Delay          : 20
  Bridge Hello Time             : 05
  Bridge Max Age                : 30
  Root Port                     : 0
  Root Path Cost                : 0
  Designated Root               : 80:00:00:20:06:25:ed:89
  Designated Root Priority      : 0
  Root Bridge Forward Delay     : 20
  Root Bridge Hello Time        : 05
  Root Bridge Max Age           : 30
  Topology Change Count         : 0
  Time Since Topology Chg       : 567
ML2400(rstp)## exit
ML2400#
```

13.2.2 Smart RSTP (Ring-Only Mode) through the Command Line Interface

A special case of a mesh structure is a ring. In many networks, network managers prefer to create a ring structure for redundancy and simplicity of the topology. In a ring structure:

1. All switches in the network are GE Multilin switches.
2. RSTP is enabled on all the switches.
3. The topology is a ring.
4. All switches in the ring have been configured to use the Smart RSTP (ring only mode) (as shown below).
5. All switches in the ring must use the same firmware revision.

The ring structure can demonstrate fast recovery times, typically faster than what RSTP can recover from a single fault. In many situations RSTP will recover in seconds, whereas smart RSTP (ring-only mode) will recover in milliseconds.

To configure Ring-Only mode, ensure the first three of the four situations described above are met.

RSTP mode has to be enabled before any configuration to the ring-only mode.

The RSTP command enters the RSTP configuration mode and enables/disables RSTP. By default, RSTP is disabled and has to be manually activated.

rstp
rstp *<enable|disable>*

The syntax for the *romode* command on RSTP is shown below.

romode add port=<port|list|range>
romode del port=<port|list|range>
romode <enable|disable>
romode show

The sequence of commands for enabling ring-only mode is shown in the following example:

Example 13-5: Configuring smart RSTP, ring-only mode

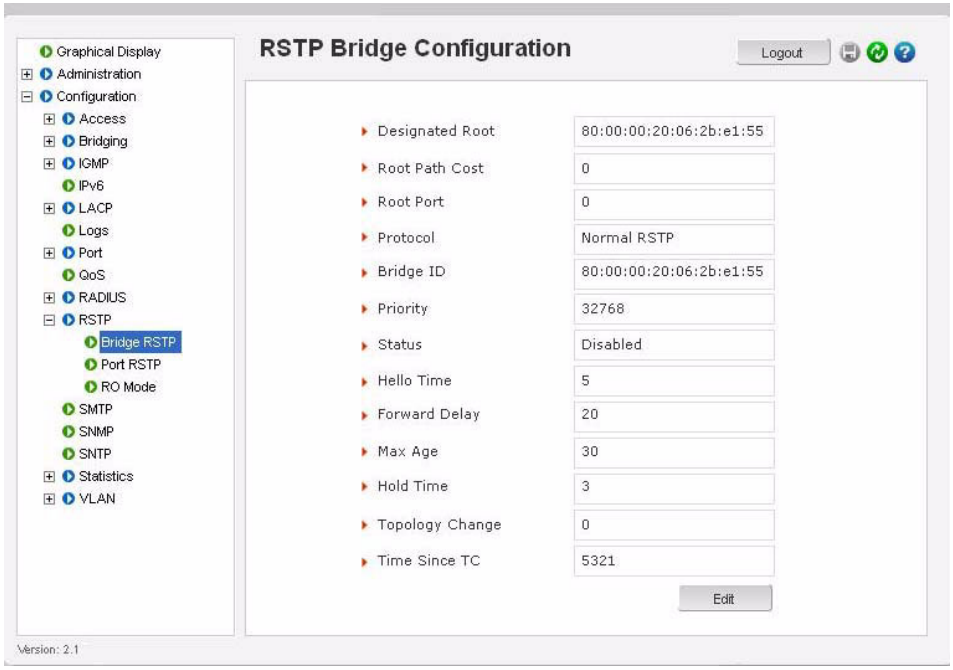
```
ML2400# rstp

ML2400(rstp)##rstp enable
Successfully set the RSTP status

ML2400(rstp)##romode show
  RO-MODE status       : Disabled
  RO-MODE set on ports : NONE

ML2400(rstp)##romode add port=1,2
        Added Ports: 1,2

ML2400(rstp)##romode enable
RSTP Ring Only Mode Enabled.

ML2400(rstp)##romode show
  RO-MODE status       : Enabled
  RO-MODE set on ports : 1,2

ML2400(rstp)##romode disable
RSTP Ring Only Mode Disabled.

ML2400(rstp)##romode show
  RO-MODE status       : Disabled
  RO-MODE set on ports : 1,2

ML2400(rstp)##romode del port=1,2
        Deleted Ports: 1,2

ML2400(rstp)##romode show
  RO-MODE status       : Disabled
  RO-MODE set on ports : NONE

ML2400(rstp)##
```

13.3 Configuring STP/RSTP with EnerVista Secure Web Management software

13.3.1 Normal RSTP

To setup and configure RSTP, select the **Configure > RSTP** menu items. In setting up RSTP or STP, it is advised that the system defaults are used for weights and other parameters. Only when specific ports are required to be the active link should the default values change.

In the window below, RSTP or STP is disabled. The designated root is set to zero as RSTP is disabled.

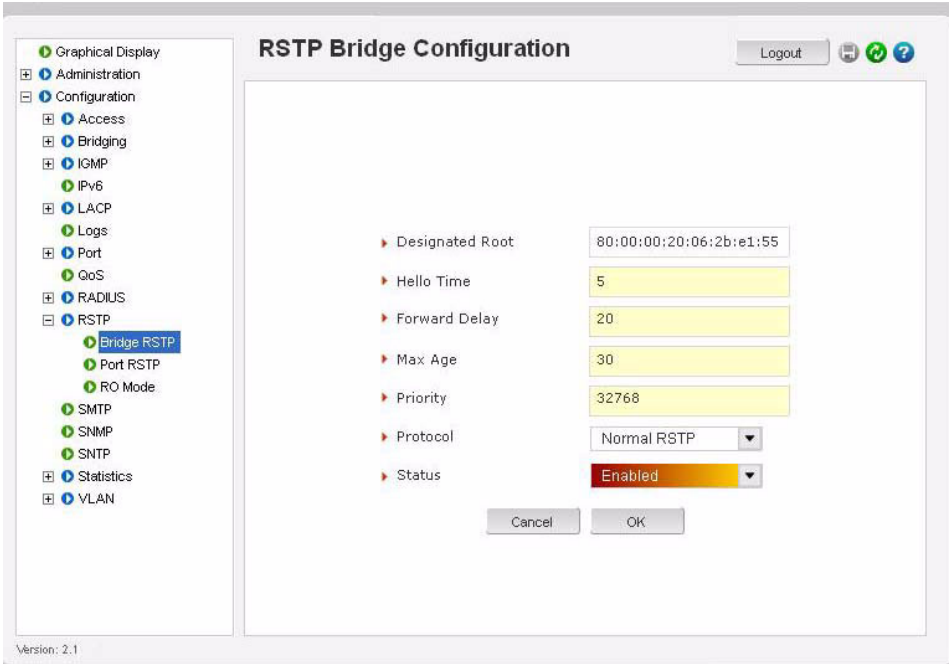


The RSTP bridge configuration parameters are defined below.

- **Designated Root**: Shows the MAC address of the bridge in the network elected or designated as the root bridge. Normally, when STP is not enabled, the switch designates itself as the root switch.
- **Root Path Cost**: A path cost is assigned to individual ports for the switch to determine which ports are the forwarding points. A higher cost means more loops; a lower cost fewer loops. More loops equal more traffic and a tree which takes a long time to converge, resulting in a slower system
- **Root Port**: Indicates the port number, which is elected as the root port of the switch. A root port of "0" indicates STP is disabled.
- **Protocol**: Indicates whether STP or RSTP is being used. It also indicates if RSTP is used in Smart RSTP (ring-only mode) or normal mode.
- **Bridge ID**: Indicates the MAC address of the current bridge over which traffic will flow.
- **Bridge Priority**: Specifies the switch (bridge) priority value. This value is used along with the switch MAC address to determine which switch in the network is the root device. Lower values mean higher priority. The value ranges from 0 to 65535, with a default of 32768

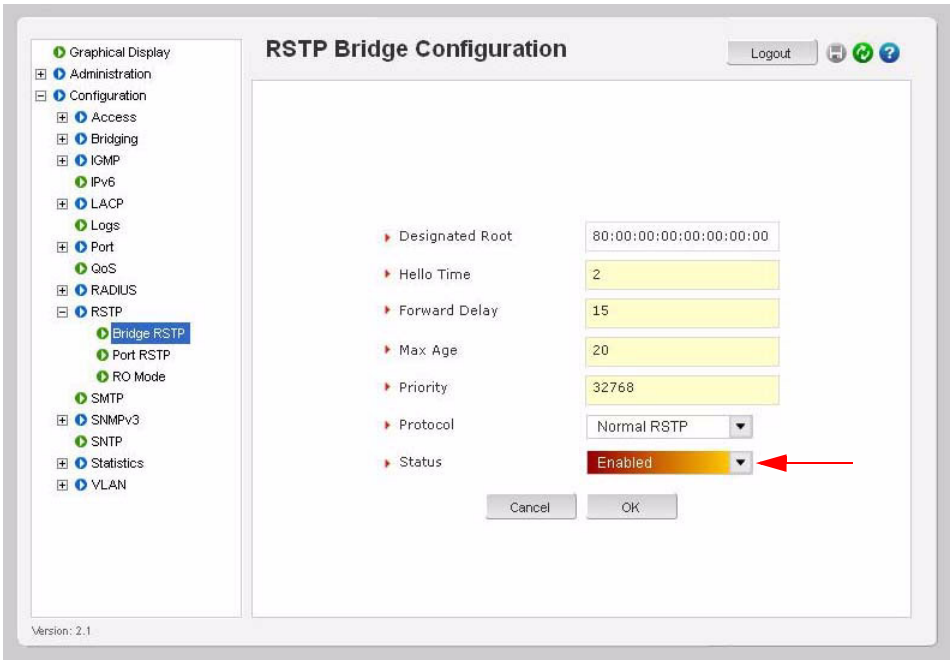
- **Status**: Indicates whether STP or RSTP is enabled.
- **Bridge Hello Time**: When the switch is the root device, this is the time between messages being transmitted. The value is from 1 to 10 seconds, with a default of 2.
- **Bridge Forward Delay**: Indicates the time duration the switch will wait from listening to learning states and from learning to forwarding states. The value ranges from 4 to 30 seconds, with a default of 15.
- **Bridge Max Age**: This is the maximum time a message with STP information is allowed by the switch before the switch discards the information and updates the address table again. The value ranges from 6 to 40 seconds with a default 20.
- **Hold Time**: This is the minimum time period to elapse between the transmissions of configuration BPDUs through a given LAN Port. At most one configuration BPDU shall be transmitted in any hold time period. This parameter is a fixed parameter, with values as specified in RSTP standard (3 seconds).
- **Topology Change**: A counter indicating the number of times topology has changed.
- **Time since TC**: Indicates time that has elapsed since the last topology change. Use this in conjunction with uptime on the graphical display (screen shown after a successful login) to find the frequency of the topology changes.

▷ Click on **Edit** to make any changes.
On this screen, you can select and enable STP or RSTP.



▷ Under protocol, select “Force to STP” if there are legacy or other third party devices that do not support RSTP.

▷ Otherwise it is recommended to enable “Normal RSTP”.

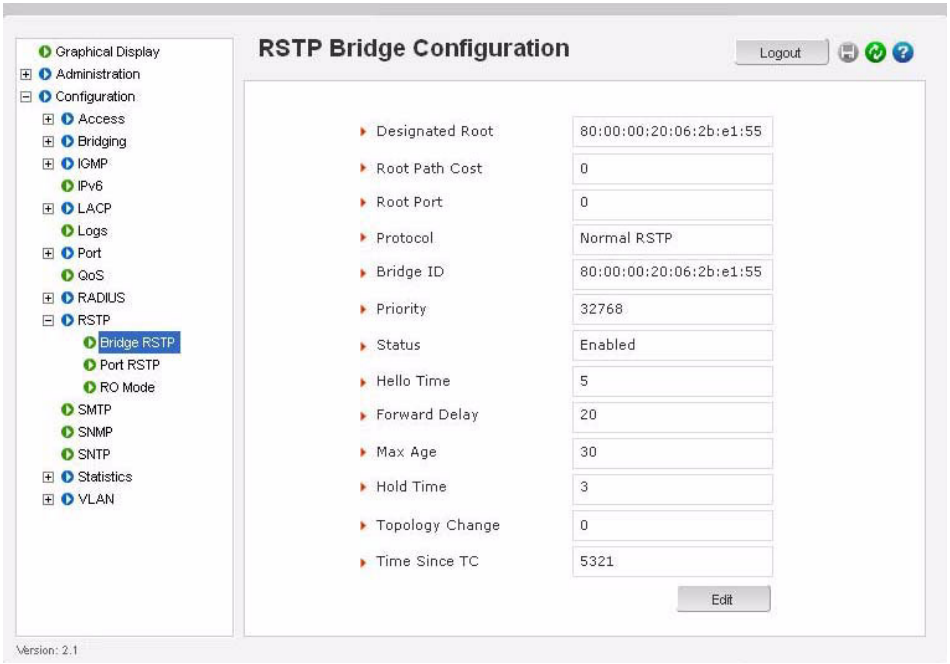


Once again, if you are not familiar with the STP or RSTP parameter settings, is best to use the default values.

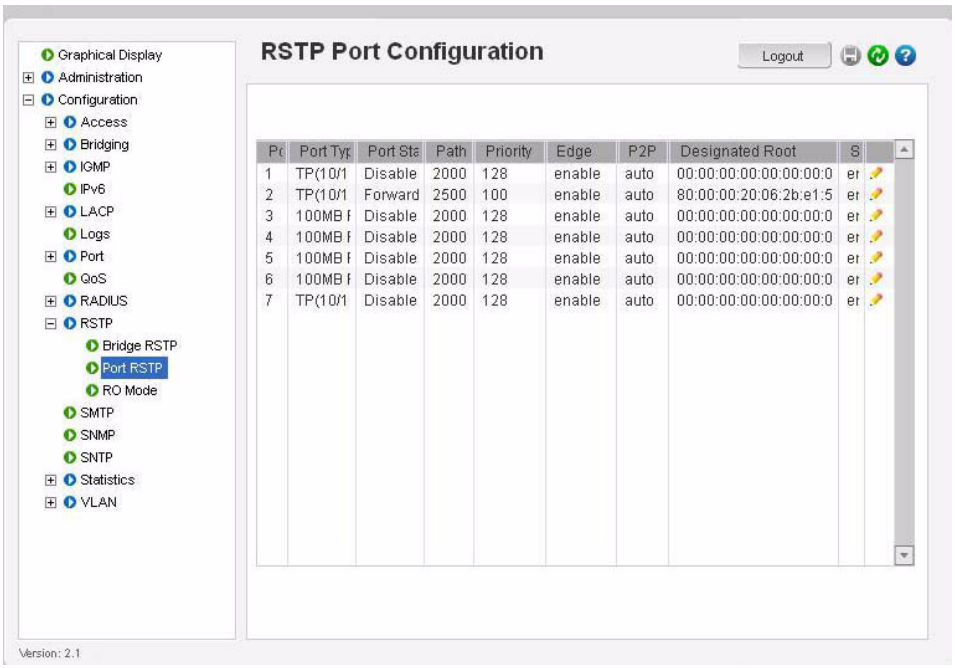
▷ **Simply enable RSTP (or STP) and let the system default values prevail.**

After RSTP is enabled, the fields are updated.

▷ Note the **Status**, **Time since TC**, and **Designated Root** values.



The port specific values for RSTP or STP are shown below.



▷ **Click on the edit icon ( ) to edit the values for a specific port.**

The columns in the above window are defined as follows:

- **Port#**: Indicates the port number. Value ranges from 1 to the maximum number of ports in the switch.
- **Port Type**: Indicates the type of port and speed; TP indicates twisted-pair.
- **Port State**: Forwarding implies traffic is forwarded onto the next switch or device connected the port. Disabled implies that the port may be turned off or the device connected to it may be unplugged or turned off. Values can be Listening, Learning, Forwarding, Blocking and Disabled.
- **Path Cost**: This is the assigned port cost value used for the switch to determine the forwarding points. Values range from 1 to 2000000. The lower the value, the lower the cost and hence the preferred route. The costs for different Ethernet speeds are shown below. The STP path cost is compared to the RSTP path cost.

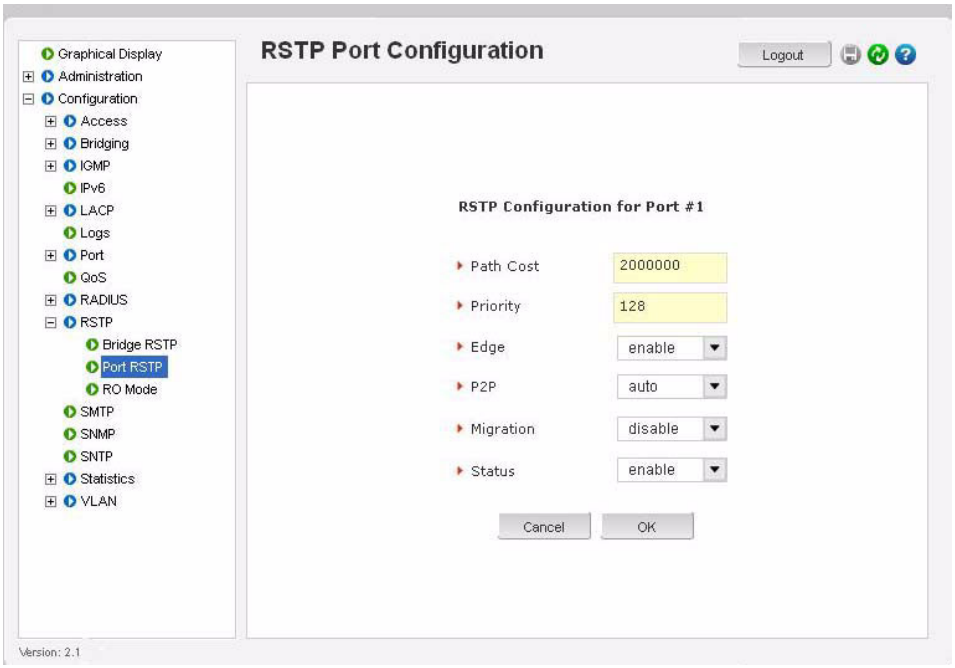
Table 13–2: Path cost defined in IEEE 802.1d and 802.1w

Port Type	STP Path cost	RSTP Path cost
10 Mbps	100	2 000 000
100 Mbps	19	200 000
1 Gbps	4	20 000
10 Gbps	2	2000

- **Priority**: STP uses this to determine which ports are used for forwarding. Lower the number means higher priority. Value ranges from 0 to 255. Default is 128
- **Edge Ports**: RSTP offers edge port recognition, allowing ports at the edge of the network to forward frames immediately after activation while at the same time protecting them against loops.

- **P2P Ports**: set the "point-to-point" value to off on all ports that are connected to shared LAN segments (i.e. connections to hubs). The default value is auto. P2P ports would typically be end stations or computers on the network.
- **Designated Root**: MAC Address of the Root Bridge in the tree
- **Status**: status of STP/RSTP for the port.

The STP or RSTP values can be changed for each port as shown below.



Migration is enabled for all ports connected to other devices such as hubs, bridges and switches known to support IEEE 802.1d STP services and cannot support RSTP services.

Status is normally enabled - in certain cases the Status can be set to disabled to turn off RSTP or STP on that port.

13.3.2 Smart RSTP (Ring-Only Mode) with EnerVista Secure Web Management Software

A ring is a special case mesh structure. In many networks, network managers prefer to create a ring structure for topological redundancy and simplicity. In a ring structure:

1. All switches in the network are GE Multilin switches.
2. RSTP is enabled on all the switches.
3. The topology is a ring.
4. All switches in the ring have been configured to use the ring-only mode (as shown below).
5. All switches in the ring myst use the same firmware revision.

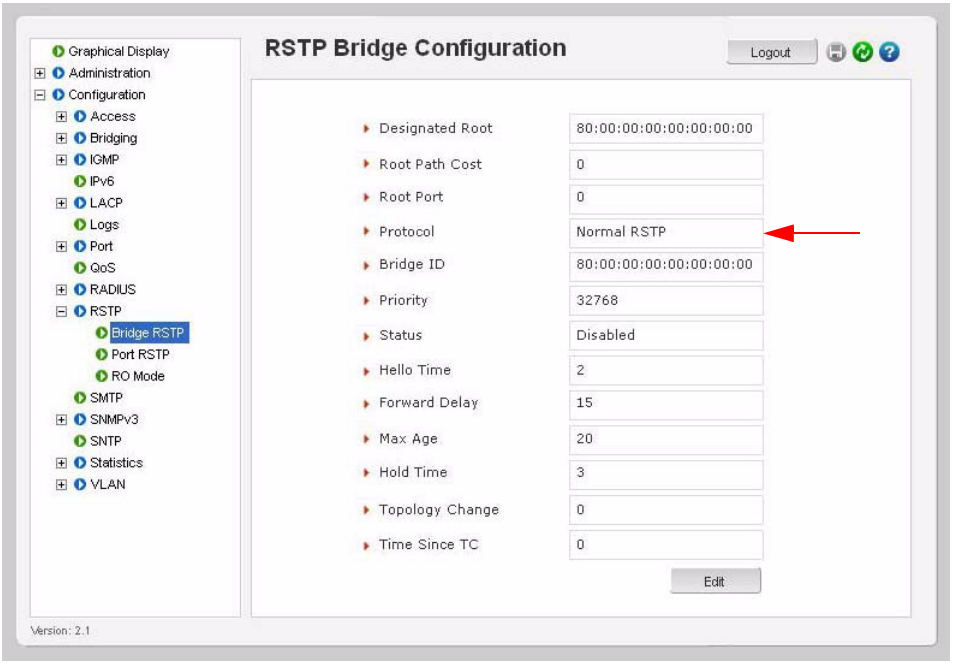
The ring structure can demonstrate fast recovery times, typically faster than what RSTP can recover from a single fault. In many situations RSTP will recover in seconds, whereas smart RSTP (Ring-Only mode) will recover in milliseconds.

To configure ring-only mode, ensure the first three of the four situations described above are met.

To enable ring-only mode, first

▷ Enable RSTP by setting the **STP Type** to RSTP in the **Administration > Set > STP Type** menu:

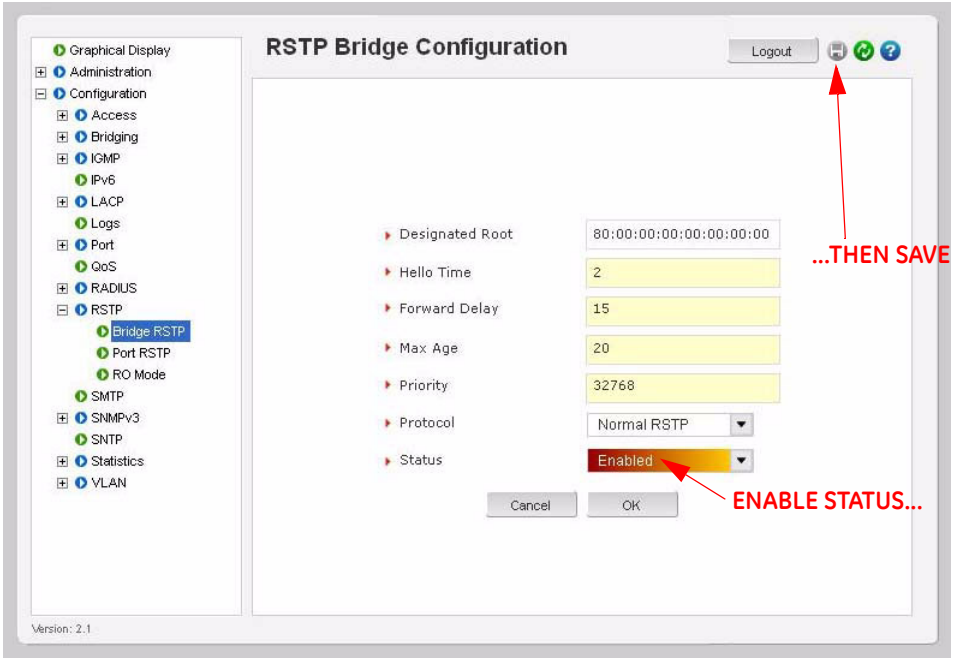
▷ Select the **Configuration > RSTP > Bridge RSTP** menu as shown below.



▷ Click the Edit button to configure RSTP.

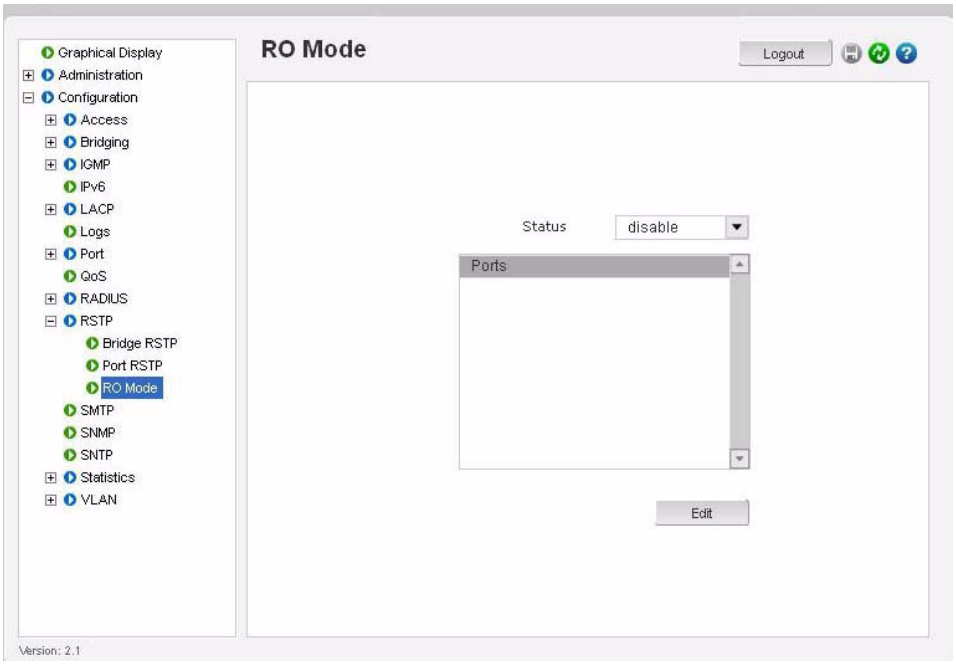
▷ Once in Edit mode, change the Status to Enable.

▷ Save Configuration.



To reset RSTP back to normal mode, select "Normal RSTP" for the **Protocol** setting. Save the configuration by clicking on the icon.

▷ Select the **Configuration > RSTP > RO Mode** menu as shown below:

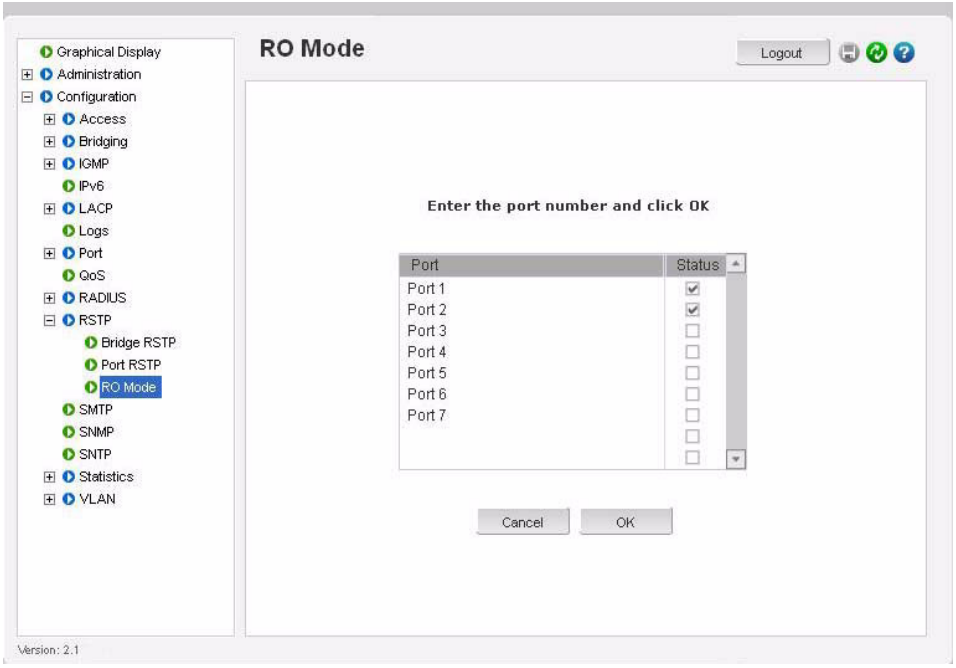


▷ Click the **Edit** button to configure RO Mode.

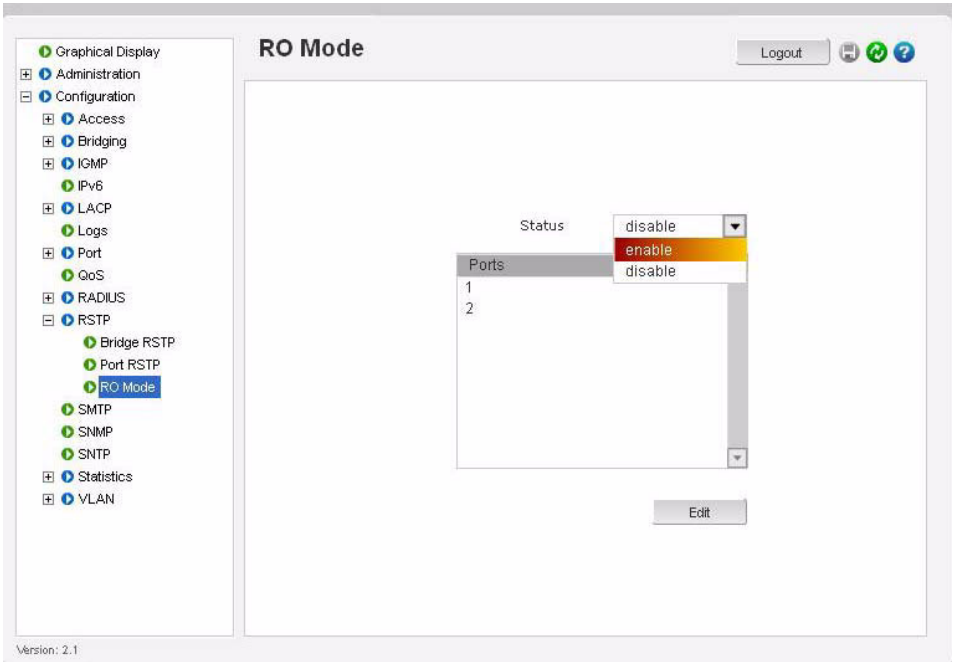
▷ Select the desired ports as shown below, then click **OK** to exit.

NOTE

Only 2 ports can be selected to Ring Only Mode.



▷ Select the **Enabled** option for the Status setting as shown below:



▷ Save the configuration by clicking on the icon.

Multilink ML2400

Ethernet Communications Switch

Chapter 14: Quality of Service

14.1 QoS Overview

14.1.1 Description

Quality of Service (QoS) refers to the capability of a network to provide different priorities to different types of traffic. Not all traffic in the network has the same priority. Being able to differentiate different types of traffic and allowing this traffic to accelerate through the network improves the overall performance of the network and provides the necessary quality of service demanded by different users and devices. The primary goal of QoS is to provide priority including dedicated bandwidth.

14.1.2 QoS Concepts

The MultiLink family of switches supports QoS as specified in the IEEE 802.1p and IEEE 802.1q standards. QoS is important in network environments where there are time-critical applications, such as voice transmission or video conferencing, which can be adversely effected by packet transfer delays or other latency in a network.

Most switches today implement buffers to queue incoming packets as well as outgoing packets. In a queue mechanism, normally the packet which comes in first leaves first (FIFO) and all the packets are serviced accordingly. Imagine, if each packet had a priority assigned to it. If a packet with a higher priority than other packets were to arrive in a queue, the packet would be given a precedence and moved to the head of the queue and would go out as soon as possible. The packet is thus preempted from the queue and this method is called preemptive queuing.

Preemptive queuing makes sense if there are several levels of priorities, normally more than two. If there are too many levels, then the system has to spend a lot of time managing the preemptive nature of queuing. IEEE 802.1p defines and uses eight levels of priorities. The eight levels of priority are enumerated 0 to 7, with 0 the lowest priority and 7 the highest.

To make the preemptive queuing possible, most switches implement at least two queue buffers. The MultiLink family of switches has two priority queues, 1 (low) and 0 (high).When tagged packets enter a switch port, the switch responds by placing the packet into one of the two queues, and depending on the precedence levels the queue could be rearranged to meet the QoS requirements.

14.1.3 DiffServ and QoS

QoS refers to the level of preferential treatment a packet receives when it is being sent through a network. QoS allows time sensitive packets such as voice and video, to be given priority over time insensitive packets such as data. Differentiated Services (DiffServ or DS) are a set of technologies defined by the IETF (Internet Engineering Task Force) to provide quality of service for traffic on IP networks.

DiffServ is designed for use at the edge of an Enterprise where corporate traffic enters the service provider environment. DiffServ is a layer-3 protocol and requires no specific layer-2 capability, allowing it to be used in the LAN, MAN, and WAN. DiffServ works by tagging each packet (at the originating device or an intermediate switch) for the requested level of service it requires across the network.

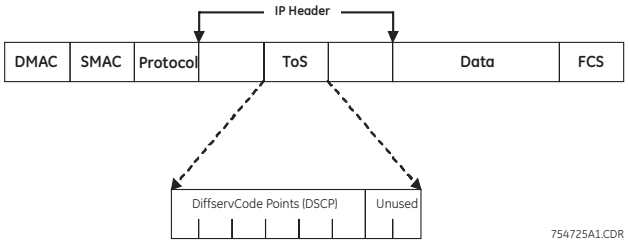


FIGURE 14–1: ToS and DSCP

DiffServ inserts a 6-bit DiffServ code point (DSCP) in the Type of Service (ToS) field of the IP header, as shown in the picture above. Information in the DSCP allows nodes to determine the Per Hop Behavior (PHB), which is an observable forwarding behavior for each packet. Per hop behaviors are defined according to:

- Resources required (e.g., bandwidth, buffer size)
- Priority (based on application or business requirements)
- Traffic characteristics (e.g., delay, jitter, packet loss)

Nodes implement PHBs through buffer management and packet scheduling mechanisms. This hop-by-hop allocation of resources is the basis by which DiffServ provides quality of service for different types of communications traffic.

14.1.4 IP Precedence

IP Precedence utilizes the three precedence bits in the IPv4 header's Type of Service (ToS) field to specify class of service for each packet. You can partition traffic in up to eight classes of service using IP precedence. The queuing technologies throughout the network can then use this signal to provide the appropriate expedited handling.

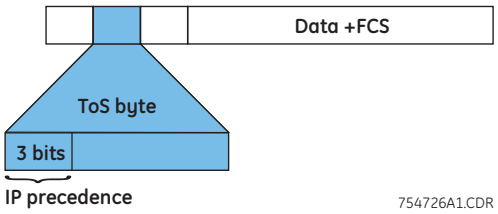


FIGURE 14–2: IP Precedence ToS Field in an IP Packet Header

The three most significant bits (correlating to binary settings 32, 64, and 128) of the Type of Service (ToS) field in the IP header constitute the bits used for IP precedence. These bits are used to provide a priority from 0 to 7 for the IP packet.

Because only three bits of the ToS byte are used for IP precedence, you need to differentiate these bits from the rest of the ToS byte.

The MultiLink family of switches has the capability to provide QoS at Layer 2. At Layer 2, the frame uses Type of Service (ToS) as specified in IEEE 802.1p. ToS uses 3 bits, just like IP precedence, and maps well from Layer 2 to layer 3, and vice versa.

The switches have the capability to differentiate frames based on ToS settings. With two queues present - high or low priority queues or buffers in MultiLink family of switches, frames can be placed in either queue and serviced via the weight set on all ports. This placement of queues, added to the weight set plus the particular tag setting on a packet allows each queue to have different service levels.

MultiLink QoS implementations provide mapping of ToS (or IP precedence) to Class of Service (CoS). A CoS setting in an Ethernet Frame is mapped to the ToS byte of the IP packet, and vice versa. A ToS level of 1 equals a CoS level of 1. This provides end-to-end priority for the traffic flow when MultiLink switches are deployed in the network.

Not all packets received on a port have high priority. IGMP and BPDU packets have high priority by default.

The MultiLink family of switches has the capability to set the priorities based on three different functions. They are

- **Port QoS**: assigns a high priority to all packets received on a port, regardless of the type of packet.
- **TAG QoS**: if a packet contains a tag, the port on which the packet was received then looks to see at which level that tag value is set. Regardless of the tag value, if there is a tag, that packet is automatically assigned high priority (sent to the high priority queue)
- **ToS QoS**: (Layer 3) when a port is set to ToS QoS, the most significant 6-bits of the IPv4 packet (which has 64 bits) are used. If the 6 bits are set to ToS QoS for the specific port number the packet went to, that packet is assigned high priority by that port

14.2 Configuring QoS through the Command Line Interface

14.2.1 Commands

MultiLink switches support three types of QoS - Port based, Tag based and ToS based.

QoS is disabled by default on the switch. QoS needs to be enabled and configured.

The `qos` command enters the QoS configuration mode.

qos

The usage of the `setqos` command varies depending on the type of QOS. For example, for QOS type tag, the tag levels have to be set, and for QOS type ToS, the ToS levels have to be set. If the priority field is not set, it then defaults to low priority. ToS has 64 levels and the valid values are 0-63 and a tagged packet has 8 levels and the valid values are 0-7

setqos *type=<port|tag|tos|none> port=<port|list|range> [priority=<high|low>] [tos=<0-63|list|range>]*
[tag=<0-7|list|range>]

Setting the `type` parameter to none will clear the QoS settings.

The `set-weight` command sets the port priority weight for All the ports. Once the weight is set, all the ports will be the same weight across the switch. The valid value for weight is 0-7

set-weight *weight=<0-7>*

A weight is a number calculated from the IP precedence setting for a packet. This weight is used in an algorithm to determine when the packet will be serviced

The `show-portweight` command displays the weight settings on a port.

show-portweight

As mentioned previously, the switch is capable of detecting higher-priority packets marked with precedence by the IP forwarder and can schedule them faster, providing superior response time for this traffic. The IP Precedence field has values between 0 (the default) and 7. As the precedence value increases, the algorithm allocates more bandwidth to that traffic to make sure that it is served more quickly when congestion occurs. The MultiLink family of switches can assign a weight to each flow, which determines the transmit order for queued packets. In this scheme, lower weights (set on all ports) are provided more service. IP precedence serves as a divisor to this weighting factor. For instance, traffic with an IP Precedence field value of 7 gets a lower weight than traffic with an IP Precedence field value of 3, and thus has priority in the transmit order.

Once the port weight is set, the hardware will interpret the weight setting for all ports as outlined below (assuming the queues are sufficiently filled - if there are no packets, for example, in the high priority queue, packets are serviced on a first come first served - FCFS - basis from the low priority queue).

Table 14–1: Port weight settings

Value	Hardware traffic queue behavior
0	No priority - traffic is sent alternately from each queue and packets are queued alternately in each queue.
1	Two packets are sent from the HIGH priority queue and one packet from LOW priority queue.
2	Four packets are sent from the HIGH priority queue and one packet from LOW priority queue.
3	Six packets are sent from the HIGH priority queue and one packet from LOW priority queue.
4	Eight packets are sent from the HIGH priority queue and one packet from LOW priority queue.
5	Ten packets are sent from the HIGH priority queue and one packet from LOW priority queue.
6	Twelve packets are sent from the HIGH priority queue and one packet from LOW priority queue.
7	All packets are sent from the HIGH priority queue and none are sent from LOW priority queue.

The `show qos` command displays the QoS settings

show qos *[type=<port|tag|tos>] [port=<port|list|range>]*

Sometimes it is necessary to change the priority of the packets going out of a switch. For example, when a packet is received untagged and has to be transmitted with an addition of the 802.1p priority tag, the tag can be assigned depending on the `untag` value set. For example if the `untag` command is set to `port=1 tag=2 priority=low`, untagged packets received on that port will be tagged with a priority low upon transmit.

The `untag` command defines the 802.1p user priority assigned to untagged received packets to be transmitted as tagged from the priority queue.

set-untag *port=<port|list|range> priority=<high|low> tag=<0-7>*

14.2.2 Example

The following example shows how to configure QoS.

Example 14-1: Configuring QoS

```
ML2400# show port

Keys:  E  = Enable            D  = Disable
       H  = Half Duplex       F  = Full Duplex
       M  = Multiple VLAN's   NA = Not Applicable
       LI = Listening         LE = Learning
       F  = Forwarding        B  = Blocking

Port  Name      Control  Dplx  Media  Link  Speed  Part  Auto  VlanID  GVRP  STP
-------------------------------------------------------------------------------
 9    B1        E        H     10Tx   UP    10     No    E     1       -     -
10    B2        E        H     10Tx   DOWN  10     No    E     1       -     -
11    JohnDoe   E        H     10Tx   DOWN  10     No    E     1       -     -
12    JaneDoe   E        H     10Tx   DOWN  10     No    E     1       -     -
13    B5        E        F     100Tx  UP    100    No    E     1       -     -
14    B6        E        H     10Tx   DOWN  10     No    E     1       -     -
15    B7        E        H     10Tx   DOWN  10     No    E     1       -     -
16    B8        E        H     10Tx   DOWN  10     No    E     1       -     -

ML2400## qos
ML2400(qos)## setqos type=port port=10 priority=high
ML2400(qos)##

  Successfully set QOS.

ML2400(qos)## show qos

  ==============================
   PORT  |  QOS   |  STATUS
  ==============================
      9  |  None  |  UP
     10  |  Port  |  DOWN
     11  |  None  |  DOWN
     12  |  None  |  DOWN
     13  |  None  |  UP
     14  |  None  |  DOWN
     15  |  None  |  DOWN
     16  |  None  |  DOWN

ML2400(qos)## show qos type=port

  ================================
   PORT  |  PRIORITY  |  STATUS
  ================================
      9  |  Low       |  UP
     10  |  High      |  DOWN
     11  |  Low       |  DOWN
     12  |  Low       |  DOWN
     13  |  Low       |  UP
     14  |  Low       |  DOWN
     15  |  Low       |  DOWN
     16  |  Low       |  DOWN

ML2400(qos)## setqos port=11 priority=high type=tag tag=6

  Successfully set QOS.
```

All traffic on port 10 is sent to the high priority queue.

All traffic on port 11 is sent to the high priority queue and the QoS tag is set to 6.

(continued on next page)

Configuring QoS (continued)

```
ML2400(qos)## show qos
 ==============================
  PORT   |  QOS    |  STATUS
 ==============================
     9   |  None   |  UP
    10   |  Port   |  DOWN
    11   |  Tag    |  DOWN
    12   |  None   |  DOWN
    13   |  None   |  UP
    14   |  None   |  DOWN
    15   |  None   |  DOWN
    16   |  None   |  DOWN
ML2400(qos)## show qos type=tag
 ==============================
  PORT   |  QOS    |  STATUS
 ==============================
     9   |         |  UP
    10   |         |  DOWN
    11   |  6      |  DOWN
    12   |         |  DOWN
    13   |         |  UP
    14   |         |  DOWN
    15   |         |  DOWN
    16   |         |  DOWN
ML2400(qos)## setqos port=12 priority=high type=tag tag=5
  Successfully set QOS.
ML2400(qos)## show qos type=tag
 ==============================
  PORT   |  QOS    |  STATUS
 ==============================
     9   |         |  UP
    10   |         |  DOWN
    11   |  6      |  DOWN
    12   |  5      |  DOWN
    13   |         |  UP
    14   |         |  DOWN
    15   |         |  DOWN
    16   |         |  DOWN
ML2400(qos)## show-portweight
  Port priority Weight set to 1 High : 1 Low.
ML2400(qos)## set-weight weight=4
ML2400(qos)## show-portweight
  Port priority Weight set to 8 High : 1 Low.
```

The queue behavior is set so that 8 high-priority packets and 1 low-priority packet is sent out.

(continued on next page)

Configuring QoS (continued)

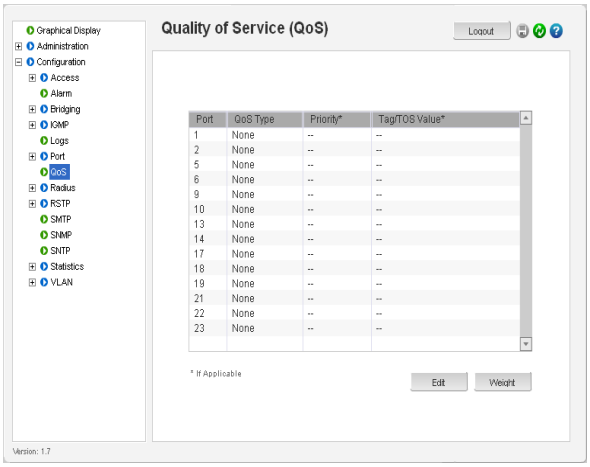
```
ML2400(qos)## show qos

  ==============================
   PORT   |  QOS    |  STATUS
  ==============================
      9   |  None   |  UP
     10   |  Port   |  DOWN
     11   |  Tag    |  DOWN
     12   |  Tag    |  DOWN
     13   |  None   |  UP
     14   |  None   |  DOWN
     15   |  None   |  DOWN
     16   |  None   |  DOWN

ML2400(qos)##
```

14.3 Configuring QoS with EnerVista Secure Web Management Software

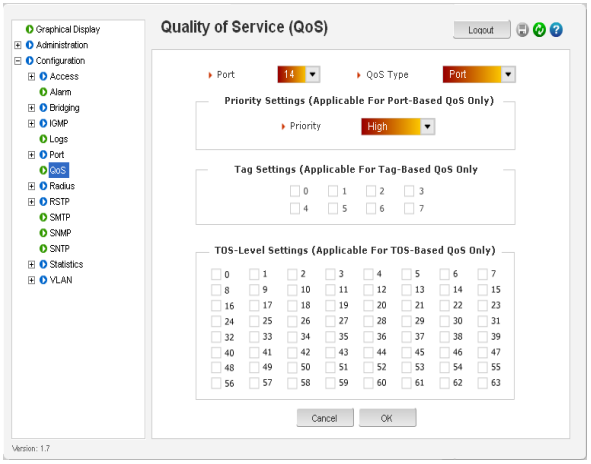
14.3.1 Description

To access QoS settings,

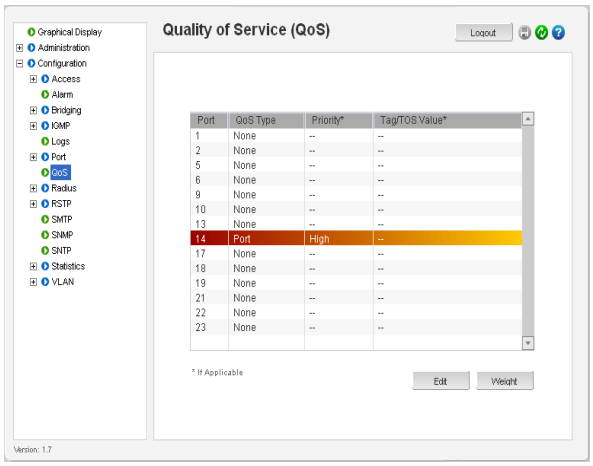
▷ Select the **Configuration > QoS** menu items.



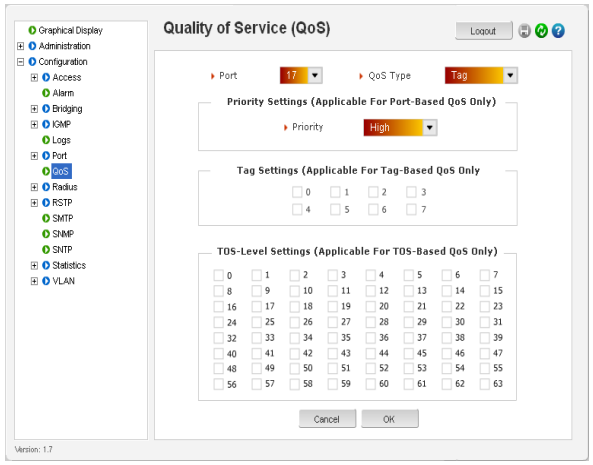
▷ Select the **Port** and the type of QoS/ToS settings.
The following window illustrates the setting of port 14 for port-based QoS with a high priority. Note the sections on Tag and TOS are ignored for Port settings.



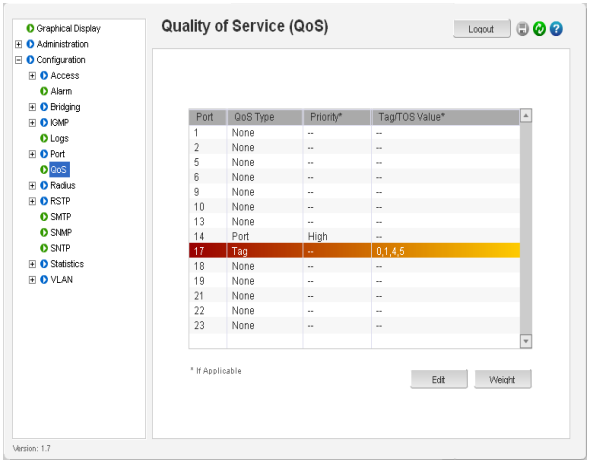
After the port QoS settings are completed, the changes are reflected on the QoS menu screen. The port 14 QoS settings indicate high priority set.



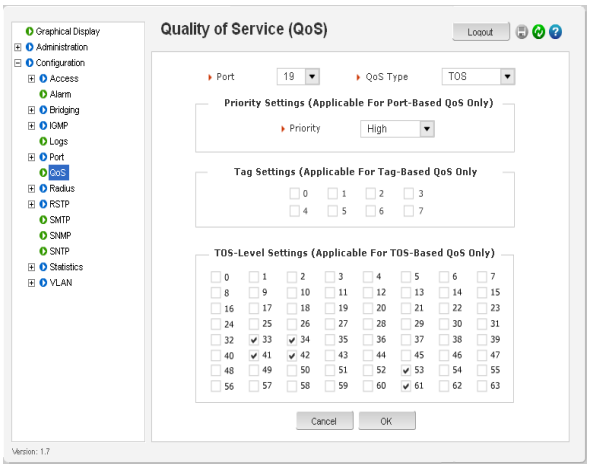
Next, a tag-based QoS is enabled on port 17. Note that only the menu area for the tag setting is relevant.



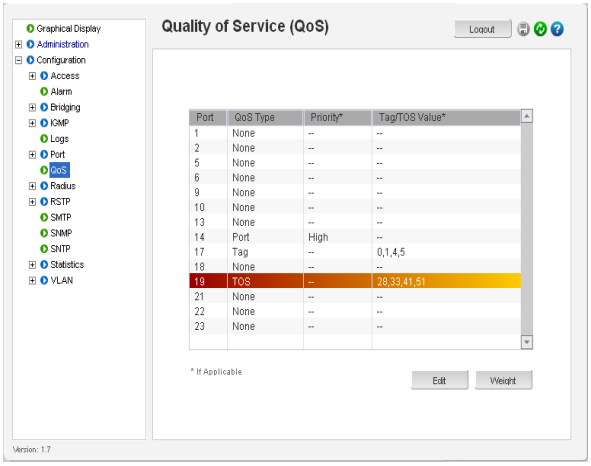
After the Tag QoS settings are completed, the changes are reflected on the QoS menu screen.



In the following window, a ToS is enabled on Port 19. As before, only the ToS level settings are relevant.



Note that the different settings are clear from the window below. Port 14 has port-based QoS, port 15 has tag-based QoS, and port 16 is using ToS.



▷ **After all changes are made, save the changes using the save icon ( ).**

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 15: IGMP

15.1 Overview

15.1.1 Description

Internet Group Management Protocol (IGMP) is defined in RFC 1112 as the standard for IP multicasting in the Internet. It is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allows a host to inform its local router, using Host Membership Reports that it wants to receive messages addressed to a specific multicast group. All hosts conforming to level 2 of the IP multicasting specification require IGMP.

15.1.2 IGMP Concepts

The ML2400 supports IGMP L2 standards as defined by RFC 1112. IGMP is disabled by default and needs to be enabled on the MultiLink family of switches. IP multicasting is defined as the transmission of an IP datagram to a “host group”, a set of zero or more hosts identified by a single IP destination address. A multicast datagram is delivered to all members of its destination host group with the same “best-efforts” reliability as regular unicast IP datagrams, i.e. the datagram is not guaranteed to arrive at all members of the destination group or in the same order relative to other datagrams.

The membership of a host group is dynamic; that is, hosts may join and leave groups at any time. There is no restriction on the location or number of members in a host group, but membership may be restricted to only those hosts possessing a private access key. A host may be a member of more than one group at a time. A host need not be a member of a group to send datagrams to it.

A host group may be permanent or transient. A permanent group has a well-known, administratively assigned IP address. It is the address and not the membership that is permanent – at any time, a permanent group may have any number of members, even

zero. On the other hand, a transient group is dynamically assigned an address when the group is created, at the request of a host. A transient group ceases to exist, and its address becomes eligible for reassignment, when its membership drops to zero.

The creation of transient groups and the maintenance of group membership is the responsibility of "multicast agents", entities that reside in internet gateways or other special-purpose hosts. There is at least one multicast agent directly attached to every IP network or sub-network that supports IP multicasting. A host requests the creation of new groups, and joins or leaves existing groups by exchanging messages with a neighboring agent.

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP (in the MultiLink implementation of IGMP, a multicast router is not necessary as long as a switch is configured to support IGMP with the querier feature enabled). A set of hosts, routers, and/or switches that send or receive multicast data streams to or from the same source(s) is termed a multicast group, and all devices in the group use the same multicast group address. The multicast group running version 2 of IGMP uses three fundamental types of messages to communicate:

- **Query**: A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network (if you need to disable the querier feature, you can do so using the IGMP configuration MIB).
- **Report**: A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
- **Leave Group**: A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group. Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

When IGMP is enabled on the MultiLink family of switches, it examines the IGMP packets it receives to:

- Learn which ports are linked to IGMP hosts and multicast routers/queriers belonging to any multicast group.
- Become a querier if a multicast router/querier is not discovered on the network.

Once the switch learns the port location of the hosts belonging to any particular multicast group, it can direct group traffic to only those ports, resulting in bandwidth savings on ports where group members do not reside. The following example illustrates this operation.

The figure below shows a network running IGMP.

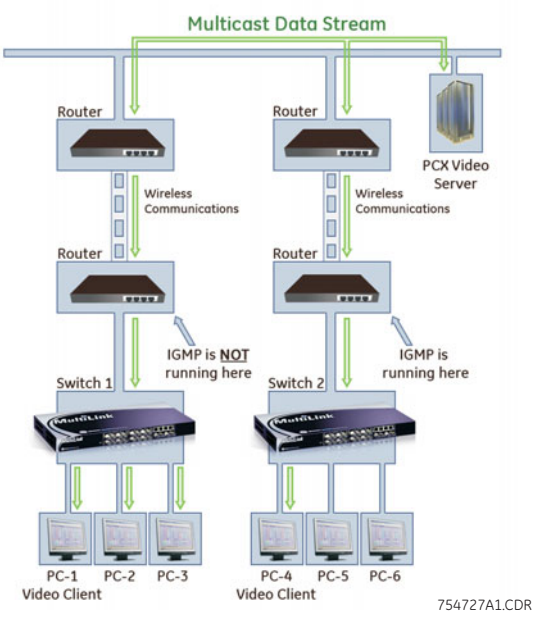


FIGURE 15–1: Advantages of using IGMP

In the above diagram:

- PCs 1 and 4, switch 2, and all of the routers are members of an IP multicast group (the routers operate as queriers).
- Switch 1 ignores IGMP traffic and does not distinguish between IP multicast group members and non-members. Thus, sends large amounts of unwanted multicast traffic to PCs 2 and 3.
- Switch 2 is recognizing IGMP traffic and learns that PC 4 is in the IP multicast group receiving multicast data from the video server (PC X). Switch 2 then sends the multicast data only to PC 4, thus avoiding unwanted multicast traffic on the ports for PCs 5 and 6.

The next figure (below) shows a network running IP multicasting using IGMP without a multicast router. In this case, the IGMP-configured switch runs as a querier. PCs 2, 5, and 6 are members of the same IP multicast group. IGMP is configured on switches 3 and 4.

Either of these switches can operate as querier because a multicast router is not present on the network. (If an IGMP switch does not detect a querier, it automatically assumes this role, assuming the querier feature is enabled-the default-within IGMP.)

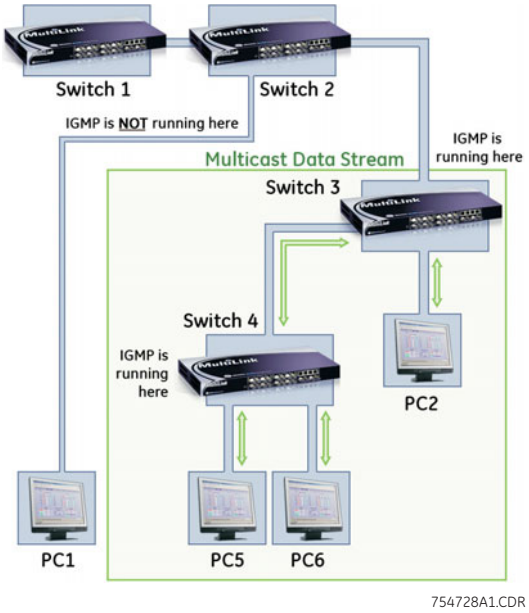


FIGURE 15–2: Isolating multicast traffic in a network

In the above figure, the multicast group traffic does not go to switch 1 and beyond. This is because either the port on switch 3 that connects to switch 1 has been configured as blocked or there are no hosts connected to switch 1 or switch 2 that belong to the multicast group.

For PC 1 to become a member of the same multicast group without flooding IP multicast traffic on all ports of switches 1 and 2, IGMP must be configured on both switches 1 and 2, and the port on switch 3 that connects to switch 1 must be unblocked.

15.1.3 IP Multicast Filters

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff in hexadecimal.) Devices such as the MultiLink family of switches having static Traffic/Security filters configured with a "Multicast" filter type and a "Multicast Address" in this range will continue in effect unless IGMP learns of a multicast group destination in this range. In that case, IGMP takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the static filter resumes control over traffic to the multicast address formerly controlled by IGMP.

15.1.4 Reserved Addresses Excluded from IP Multicast (IGMP) Filtering

Traffic to IP multicast groups in address range 224.0.0.0 to 224.0.0.255 will always be flooded because addresses in this range are “well known” or “reserved”. Thus, if IP Multicast is enabled and there is an IP multicast group within the reserved address range, traffic to that group will be flooded instead of filtered by the switch.

15.1.5 IGMP Support

The MultiLink family of switches support IGMP version 1 and version 2. The switch can act either as a querier or a nonquerier. The querier router periodically sends general query messages to solicit group membership information. Hosts on the network that are members of a multicast group send report messages. When a host leaves a group, it sends a leave group message. The difference between Version 1 and Version 2 is that version 1 does not have a “Leave” mechanism for the host. The MultiLink family of switches do pruning when there is a leave message or a time expires on a port, we prune the multicast group membership on that port.

1. The MultiLink switch supports only the default VLAN. It can be enabled within a port VLAN, tagged VLAN, or no VLAN. It can snoop up to 256 multi-cast Groups.
2. IGMP is disabled as a default. It has to be enabled to leverage the benefits of IGMP.
3. The MultiLink switch supports only the default VLAN. It can be enabled within a port VLAN, tagged VLAN, or no VLAN. It can snoop up to 256 multi-cast Groups.
4. IGMP works only on default VLAN (DEFAULT_VLAN or VID = 1).

15.2 Configuring IGMP through the Command Line Interface

15.2.1 Commands

The `igmp` command enters IGMP configuration mode and enables or disables IGMP on the switch.

igmp
igmp *<enable/disable>*

The `show igmp` command displays the IGMP status.

show igmp

The following command sequence illustrates how to enable and query the status of IGMP.

ML2400# `igmp`

ML2400(igmp)## `igmp enable`

```
IGMP is enabled
```

ML2400(igmp)## `show igmp`

```
IGMP State                    : Enabled
ImmediateLeave                : Disabled
Querier                       : Enabled
Querier Interval              : 125
Querier Response Interval     : 10
Multicasting Unknown Streams  : Enable
```

ML2400(igmp)## `igmp disable`

```
IGMP is disabled
```

ML2400(igmp)## `show igmp`

```
IGMP State                    : Disabled
ImmediateLeave                : Disabled
Querier                       : Enabled
Querier Interval              : 125
Querier Response Interval     : 10
Multicasting Unknown Streams  : Enable
```

ML2400(igmp)##

The output of the `show igmp` command provides the following useful information:

- **IGMP State** shows if IGMP is turned on (Enable) or off (Disable).
- **Immediate Leave** provides a mechanism for a particular host that wants to leave a multicast group. It disables the port (where the leave message is received) ability to transmit multicast traffic.
- **Querier** shows where the switch is a querier or a non-querier. In our example, the switch is the querier.
- **Querier Interval** shows the time period in seconds on which the switch sends general host-query messages.
- **Querier Response Interval** specifies maximum amount of time in seconds that can elapse between when the querier sends a host-query message and when it receives a response from a host.
- **Multicasting Unknown Streams** shows if the control of multicast streams is on (Enabled) or off (Disabled).

The `show-group` command displays the multicast groups.

show-group

The following command sequence illustrates how to display IGMP groups:

```
ML2400(igmp)## show-group
  GroupIp      PortNo  Timer  LeavePending
  ---------------------------------------
  224.1.0.1    9       155    0
  224.0.1.40   9       155    0
ML2400(igmp)##
```

The output of the `show-group` command displays the following information:

- **Group IP** column shows the multicast groups.
- **Port No** shows the port where the multicast group is being detected.
- **Timer** shows the amount of time left in seconds before the group port will be deleted (or will not be able to route multicast traffic) if the switch does not receive a membership report.
- **Leave Pending** column shows the number of leave messages received from this port

Every port can be individually set to three different IGMP modes - auto, block and forward.

- **Auto** - lets IGMP control whether the port should or should not participate sending multicast traffic
- **Block** - manually configures the port to always block multicast traffic
- **Forward** - manually configures the port to always forward multicast traffic

To set the port characteristics, use the `set-port` command in the IGMP configuration mode.

set-port *port=< port|list|range> mode=<auto|forward|block>*

The `show-port` command displays the port characteristics for IGMP.

show-port

The `show-router` command displays detected IGMP-enabled router ports.

show-router

The `set-leave` command enables or disables the switch to immediately process a host sending a leave message rather that wait for the timer to expire.

set-leave *<enable|disable>*

The `set-querier` command enables or disables a switch as IGMP querier.

set-querier *<enable|disable>*

The `set-qi` command sets the IGMP querier router to periodically send general host-query messages. These messages are sent to ask for group membership information. This is sent to the all-system multicast group address, 224.0.0.1. The valid range can be from 60 to 127 seconds, with a default of 125.

set-qi *interval=<value>*

The `set-qri` command sets the query response interval representing the maximum amount of time that can elapse between when the querier router sends a host-query message and when it receives a response from a host. The range can be from 2 to 270 seconds, with a default of 10. Restrictions apply to the maximum value because of an internal calculation that is dependent on the value of the query interval.

set-qri *interval=<value>*

15.2.2 Example

The following example shows how to configure IGMP.

Example 15-1: Configuring IGMP

```
ML2400(igmp)## set-port port=10-12 mode=forward
  Port mode is set.
ML2400(igmp)## show-port
  ---------------------
   Port   |  Mode
  ---------------------
   09     |  Auto
   10     |  Forwarding
   11     |  Forwarding
   12     |  Forwarding
   13     |  Auto
   14     |  Auto
   15     |  Auto
   16     |  Auto
ML2400(igmp)## show-router
  RouterIp          PortNo    Timer
  --------------------------------
  10.21.1.250          9      25
```

(continued on next page)

Configuring IGMP (continued)

```
ML2400(igmp)## set-leave enable

  IGMP immediate leave status is enabled

ML2400(igmp)## show igmp

  IGMP State                    : Enabled
  ImmediateLeave                : Enabled
  Querier                       : Enabled
  Querier Interval              : 125
  Querier Response Interval     : 10
  Multicasting Unknown Streams  : Enabled

ML2400(igmp)## set-leave disable

  IGMP immediate leave status is disabled

ML2400(igmp)## show igmp

  IGMP State                    : Enabled
  ImmediateLeave                : Disabled
  Querier                       : Enabled
  Querier Interval              : 125
  Querier Response Interval     : 10
  Multicasting Unknown Streams  : Enabled

ML2400(igmp)## set-querier enable

  IGMP querier status is enabled

ML2400(igmp)## show igmp

  IGMP State                    : Enabled
  ImmediateLeave                : Disabled
  Querier                       : Enabled
  Querier Interval              : 125
  Querier Response Interval     : 10
  Multicasting Unknown Streams  : Enabled

ML2400(igmp)## set-querier disable

  IGMP querier status is disabled

ML2400(igmp)## show igmp

  IGMP State                    : Enabled
  ImmediateLeave                : Disabled
  Querier                       : Disabled
  Querier Interval              : 125
  Querier Response Interval     : 10
  Multicasting Unknown Streams  : Enabled

ML2400(igmp)## set-qi interval=127

  Query interval successfully set

ML2400(igmp)## show igmp

  IGMP State                    : Enabled
  ImmediateLeave                : Disabled
  Querier                       : Disabled
  Querier Interval              : 127
  Querier Response Interval     : 10
  Multicasting Unknown Streams  : Enabled

ML2400(igmp)## set-qri interval=11

  Query response interval successfully set
```

(continued on next page)

Configuring IGMP (continued)

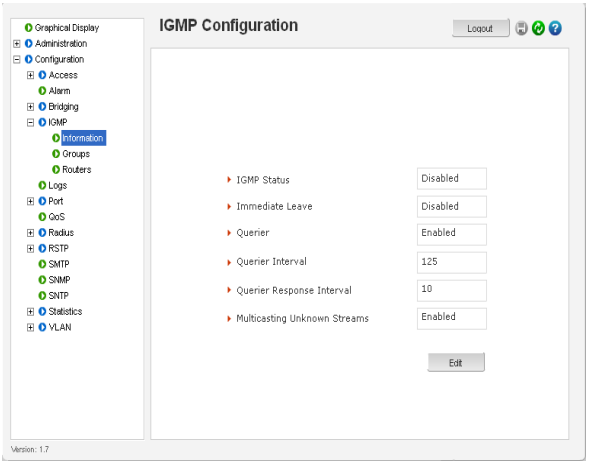
```
ML2400(igmp)## show igmp

  IGMP State                    : Enabled
  ImmediateLeave                : Disabled
  Querier                       : Disabled
  Querier Interval              : 127
  Querier Response Interval     : 11
  Multicasting Unknown Streams  : Enabled

ML2400(igmp)## mcast disable

  MCAST is disabled

ML2400(igmp)## show igmp

  IGMP State                    : Enabled
  ImmediateLeave                : Disabled
  Querier                       : Disabled
  Querier Interval              : 127
  Querier Response Interval     : 11
  Multicasting Unknown Streams  : Disabled

ML2400(igmp)## mcast enable

  MCAST is enabled

ML2400(igmp)## show igmp

  IGMP State                    : Enabled
  ImmediateLeave                : Disabled
  Querier                       : Disabled
  Querier Interval              : 127
  Querier Response Interval     : 11
  Multicasting Unknown Streams  : Enabled
```

15.3 Configuring IGMP with EnerVista Secure Web Management Software

15.3.1 Example

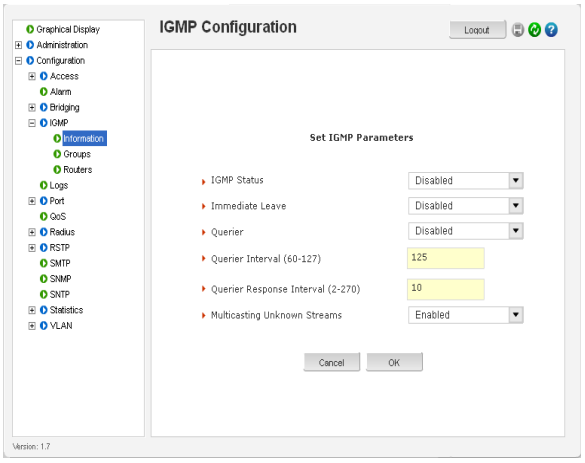
For configuring IGMP,

▷ Select the **Configuration > IGMP** menu item.
The menu allows the IGMP parameters to be set and provides information on IGMP groups and routers.



The menu allows the IGMP parameters described earlier to be set. It also provides the necessary information of IGMP groups and routers.

▷ Click on the **Edit** button to edit the IGMP parameters.
This screen also enables and disables IGMP.



Changes are reflected on the **Configuration > IGMP > Information** screen. The groups and routers screen displays the IGMP Groups and IGMP Routers information. All edits to IGMP are done through the **Information** screen.

GE Consumer & Industrial
Multilin

Multilink ML2400

Ethernet Communications Switch

Chapter 16: SNMP

16.1 Overview

16.1.1 Description

SImple Network Management Protocol (SNMP) enables management of the network. There are many software packages which provide a graphical interface and a graphical view of the network and its devices. These graphical interface and view would not be possible without SNMP. SNMP is thus the building block for network management.

16.1.2 SNMP Concepts

SNMP provides the protocol to extract the necessary information from a networked device and display the information. The information is defined and stored in a Management Information Base (MIB). MIB is the “database” of the network management information.

SNMP has evolved over the years (since 1988) using the RFC process. Several RFCs define the SNMP standards. The most common standards for SNMP are SNMP v1 (the original version of SNMP); SNMP v2 and finally SNMP v3.

SNMP is a poll based mechanism. SNMP manager polls the managed device for information and display the information retrieved in text or graphical manner. Some definitions related to SNMP are

- **Authentication** - The process of ensuring message integrity and protection against message replays. It includes both data integrity and data origin authentication
- **Authoritative SNMP engine** - One of the SNMP copies involved in network communication designated to be the allowed SNMP engine which protects against message replay, delay, and redirection. The security keys used for authenticating and encrypting SNMPv3 packets are generated as a function of the authoritative SNMP engine's engine ID and user passwords. When an SNMP message expects a response (for example, get exact, get next, set request), the receiver of these messages is

authoritative. When an SNMP message does not expect a response, the sender is authoritative

- **Community string** - A text string used to authenticate messages between a management station and an SNMP v1/v2c engine
- **Data integrity** - A condition or state of data in which a message packet has not been altered or destroyed in an unauthorized manner
- **Data origin authentication** - The ability to verify the identity of a user on whose behalf the message is supposedly sent. This ability protects users against both message capture and replay by a different SNMP engine, and against packets received or sent to a particular user that use an incorrect password or security level
- **Encryption** - A method of hiding data from an unauthorized user by scrambling the contents of an SNMP packet
- **Group** - A set of users belonging to a particular security model. A group defines the access rights for all the users belonging to it. Access rights define what SNMP objects can be read, written to, or created. In addition, the group defines what notifications a user is allowed to receive
- **Notification host** - An SNMP entity to which notifications (traps and informs) are to be sent
- **Notify view** - A view name (not to exceed 64 characters) for each group that defines the list of notifications that can be sent to each user in the group
- **Privacy** - An encrypted state of the contents of an SNMP packet where they are prevented from being disclosed on a network. Encryption is performed with an algorithm called CBC-DES (DES-56)
- **Read view** - A view name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are accessible for reading by users belonging to the group
- **Security level** - A type of security algorithm performed on each SNMP packet. The three levels are: noauth, auth, and priv. noauth authenticates a packet by a string match of the user name. auth authenticates a packet by using either the HMAC MD5 algorithms. priv authenticates a packet by using either the HMAC MD5 algorithms and encrypts the packet using the CBC-DES (DES-56) algorithm.
- **Security model** - The security strategy used by the SNMP agent. Currently, ML2400 supports three security models: SNMPv1, SNMPv2c, and SNMPv3.
- **Simple Network Management Protocol (SNMP)** - A network management protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
- **Simple Network Management Protocol Version 2c (SNMPv2c)** - The second version of SNMP, it supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.
- **SNMP engine** - A copy of SNMP that can either reside on the local or remote device.
- **SNMP group** - A collection of SNMP users that belong to a common SNMP list that defines an access policy, in which object identification numbers (OIDs) are both read-accessible and write-accessible. Users belonging to a particular SNMP group inherit all of these attributes defined by the group.

- **SNMP user** - A person for which an SNMP management operation is performed. The user is the person on a remote SNMP engine who receives the information.
- **SNMP view** - A mapping between SNMP objects and the access rights available for those objects. An object can have different access rights in each view. Access rights indicate whether the object is accessible by either a community string or a user.
- **Write view** - A view name (not to exceed 64 characters) for each group that defines the list of object identifiers (OIDs) that are able to be created or modified by users of the group.

16.2 Configuring SNMP through the Command Line Interface

16.2.1 Commands

There are several commands and variable which can be set for configuring SNMP. The basic SNMP v1 parameters can be set by referring to the section on System Parameters. Most commands here refer to SNMP v3 commands and how the variables for SNMP v3 can be configured.

The `snmp` command enters the SNMP configuration mode.

snmp

The `snmpv3` command enters the SNMP V3 configuration mode. It is still necessary to enable SNMP V3 by using the `set snmp` command after entering configuration mode.

snmpv3

The `set snmp` command defines the SNMP version. The ML2400 supports all versions (v1, v2 and v3) or only v1. By default, SNMP v1only is enabled.

set snmp *type=<v1|all>*

The `show snmp` command displays the SNMP configuration information.

show snmp

The `setvar` command sets the system name, contact and location. All parameters are optional but a user must supply at least one parameter.

setvar *[sysname|syscontact|syslocation]=<string>*

The `quickcfg` command automatically configures a default VACM (view-based access control model). This allows any manager station to access the ML2400 either via SNMP v1, v2c or v3. The community name is "public". This command is only intended for first time users and values can be changed by administrators who want more strict access.

quickcfg

The `engineid` command allows the user to change the engine ID. Every agent has to have an `engineID` (name) to be able to respond to SNMPv3 messages.

engineid *string=<string>*

The `authtrap` command enables or disables authentication traps generation.

authtrap *<enable|disable>*

The `show-authtrap` command displays the current value of authentication trap status.

show-authtrap

The `deftrap` command defines the default community string to be used when sending traps. When user does not specify the trap community name when setting a trap station using the `trap` command, the default trap community name is used.

deftrap *community=<string>*

The `show-deftrap` command displays the current value of default trap.

show-deftrap

The `trap` command defines the trap and inform manager stations. The station can receive v1, v2 traps and/or inform notifications. An inform notification is an acknowledgments that a trap has been received. A user can add up to 5 stations.

trap *<add|delete> id=<id> [type=<v1|v2|inform>] [host=<host-ip>] [community=<string>] [port=<1-65534>]*

The show-trap command shows the configured trap stations in tabular format. The `id` argument is optional and is the number corresponding to the trap entry number in the table.

show-trap *[id=<id#>]*

The `com2sec` command specifies the mapping from a source/community pair to a security name. Up to 10 entries can be specified. This part of the View based Access Control Model (VACM) as defined in RFC 2275.

com2sec *<add|delete> id=<id> [secname=<name>] [source=<source>] [community=<community>]*

The `group` command defines the mapping from sec model or a sec name to a group. A sec model is one of v1, v2c, or usm. Up to 10 entries can be specified. This part of the View based Access Control Model (VACM) as defined in RFC 2275.

group *<add|delete> id=<id> [groupname=<name>] [model=<v1|v2c|usm>] [com2secid=<com2sec-id>]*

The `show-group` command displays all or specific group entries. The `id` argument is optional and is the number corresponding to the group entry number in the table

show-group *[id=<id>]*

The `view` command defines a manager or group or manager stations what it can access inside the MIB object tree. Up to 10 entries can be specified. This part of the View based Access Control Model (VACM) as defined in RFC 2275

view *<add|delete> id=<id> [viewname=<name>] [type=<included|excluded>] [subtree=<oid>] [mask=<hex-string>]*

The `show-view` command display all or specific view entries. The `id` argument is optional and is the number corresponding to the view entry number in the table.

show-view *[id=<id>]*

The `user` command adds user entries. The ML2400 allows up to 5 users to be added. Currently, the ML2400 agent only support `noauth` and `auth-md5` for v3 authentication and `auth-des` for `priv` authentication.

user *<add|delete> id=<id> [username=<name>] [usertype=<readonly|readwrite>] [authpass=<pass-phrase>]*
[privpass=<pass-phrase>] [level=<noauth|auth|priv>] [subtree=<oid>]

The `show-user` command displays all or specific view entries. The `id` is optional and is the number corresponding to the view entry number in the table.

show-user *[id=<id>]*

16.2.2 Example

The following example shows how to configure SNMP.

Example 16-1: Configuring SNMP

```
ML2400# set snmp type=v1

  SNMP version support is set to "v1"

ML2400# show snmp

  SNMP CONFIGURATION INFORMATION
  ------------------------------
  SNMP Get Community Name  :  public
  SNMP Set Community Name  :  private
  SNMP Trap Community Name :  public
  AuthenTrapsEnableFlag    :  disabled
  SNMP Access Status       :  enabled

  SNMP MANAGERS INFO
  ------------------

  SNMP TRAP STATIONS INFO
  -----------------------

ML2400# set snmp type=all

  SNMP version support is set to "v1, v2c, v3"

ML2400# show snmp

  SNMP v3 Configuration Information

  ============================

  System Name               : ML2400
  System Location           : Markham, ON
  System Contact            : multilin.tech@ge.com
  Authentication Trap       : Disabled
  Default Trap Comm.        : public
  V3 Engine ID              : Multi_Switch_Engine

ML2400# snmpv3

ML2400(snmpv3)## setvar sysname=ml2400 syscontact=admin syslocati

ML2400(snmpv3)# quickcfg

  This will enable default VACM.
  Do you wish to proceed? ['Y' or 'N' ] Y

  Quick configuration done, default VACM enabled

ML2400(snmpv3)## engineid string=Multi_2400

  Engine ID is set successfully

ML2400(snmpv3)## authtrap enable

  Authentication trap status is set successfully

ML2400(snmpv3)## show-authtrap

  Authentication Trap Status: Enabled

ML2400(snmpv3)## deftrap community=mysecret

  Default trap community is set successfully

ML2400(snmpv3)## show-deftrap

  Default Trap Community : mysecret
```

(continued on next page)

Configuring SNMP (continued)

```
ML2400(snmpv3)## trap add id=1 type=v1 host=3.94.200.107

  Entry is added successfully

ML2400(snmpv3)## show-trap

  ID  Trap Type  Host IP          Community  Port
  ================================================
  1   v1         3.94.200.107     --         --
  2   --         --               --         --
  3   --         --               --         --
  4   --         --               --         --
  5   --         --               --         --

ML2400(snmpv3)## show-trap id=1

  Trap ID    : 1
  Trap Type  : v1
  Host IP    : 3.94.200.107
  Community  : --
  Auth. Type : --

ML2400(snmpv3)## com2sec add id=1 secname=public source=default c

  Entry is added successfully

ML2400(snmpv3)## com2sec add id=2

  ERROR: "secname" parameter is required for "add" directive

ML2400(snmpv3)## com2sec add id=2 secname=BCM

  Entry is added successfully

ML2400(snmpv3)## show-com2sec

  ID  Sec. Name       Source          Community

  ============================================

  1   public          default         public
  2   BCM             default         public
  3   --              --              --
  4   --              --              --
  5   --              --              --
  6   --              --              --
  7   --              --              --
  8   --              --              --
  9   --              --              --
  10  --              --              --

ML2400(snmpv3)## show-com2sec id=2

  Com2Sec ID    : 2
  Security Name : BCM
  Source        : default
  Community     : public

ML2400(snmpv3)## group add id=1 groupname=v1 model=v1 com2secid=1

  Entry is added successfully
```

(continued on next page)

Configuring SNMP (continued)

```
ML2400(snmpv3)## show-group
  ID  Group Name     Sec. Model     Com2Sec ID
  ================================================
  1   v1              v1            1
  2   public          v2c           1
  3   public          usm           1
  4   --              --            --
  5   --              --            --
  6   --              --            --
  7   --              --            --
  8   --              --            --
  9   --              --            --
  10  --              --            --
ML2400(snmpv3)## show-group id=1
  Group ID   : 1
  Group Name : v1
  Model      : v1
  Com2Sec ID : 1
ML2400(snmpv3)## view add id=1 viewname=all type=included subtree=.1
  Entry is added successfully
ML2400(snmpv3)## show-view
  ID  View Name      Type           Subtree  Mask
  ================================================
  1   all             included      1        ff
  2   --              --            --       --
  3   --              --            --       --
  4   --              --            --       --
  5   --              --            --       --
  6   --              --            --       --
  7   --              --            --       --
  8   --              --            --       --
  9   --              --            --       --
  10  --              --            --       --
ML2400(snmpv3)## show-view id=1
  View ID    : 1
  View Name  : all
  Type       : included
  Subtree    : .1
  Mask       : ff
ML2400(snmpv3)## access add id=1 accessname=v1 model=v1 level=noauth read=1 wr
notify=none
  Entry is added successfully
```

(continued on next page)

Configuring SNMP (continued)

```
ML2400(snmpv3)## show-access
  ID  View Name    Model     Level     R/View    W/View    N/View    Context        Prefix
  ================================================================================================
  1   v1           v1        noauth    1         none      none      ""             exact
  2   --           --        --        --        --        --        --             --
  3   --           --        --        --        --        --        --             --
  4   --           --        --        --        --        --        --             --
  5   --           --        --        --        --        --        --             --
  6   --           --        --        --        --        --        --             --
  7   --           --        --        --        --        --        --             --
  8   --           --        --        --        --        --        --             --
  9   --           --        --        --        --        --        --             --
  10  --           --        --        --        --        --        --             --
ML2400(snmpv3)## show-access id=1
  Access ID      : 1
  Access Name    : v1
  Sec. Model     : v1
  Sec. Level     : noauth
  Read View ID   : 1
  Write View ID  : none
  Notify View ID : none
  Context        : ""
  Prefix         : exact
ML2400(snmpv3)## user add id=1 username=jsmith usertype=readwrite authpass=something
  Entry is added successfully
ML2400(snmpv3)## show-user
  ID  User Name      UType      AuthPass     PrivPass     AType    Level    Subtree
  ================================================================================
  1   jsmith         RW         something    --           MD5      auth     --
  2   --             --         --           --           --       --       --
  3   --             --         --           --           --       --       --
  4   --             --         --           --           --       --       --
  5   --             --         --           --           --       --       --
ML2400(snmpv3)## show-user id=2
  ERROR: Entry is not active
ML2400(snmpv3)## show-user id=1
  User ID     : 1
  User Name   : jsmith
  User Type   : read-write
  Auth. Pass  : something
  Priv. Pass  :
  Auth. Type  : MD5
  Auth. Level : auth
  Subtree     :
ML2400(snmpv3)## exit
ML2400#
```

16.3 Configuring SNMP with EnerVista Secure Web Management Software

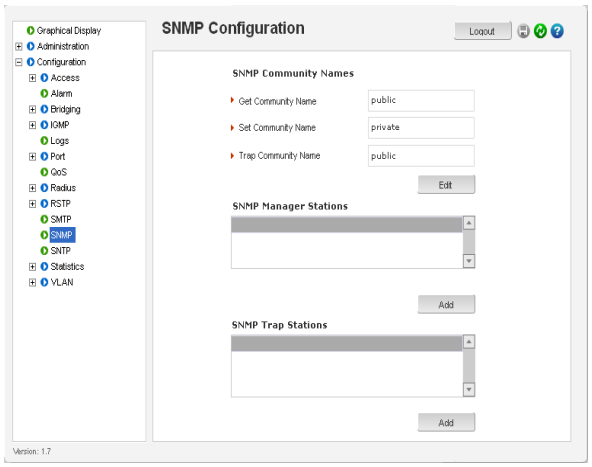
16.3.1 Example

Most SNMP v1 capabilities can be set using the EnerVista Secure Web Management Software. For SNMP v2 and v3 parameters, please refer to *Configuring SNMP through the Command Line Interface* on page 16–4.

SNMP variables are used in conjunction with Alert definitions. Alert Definitions are covered in the next chapter.

To configure SNMP,

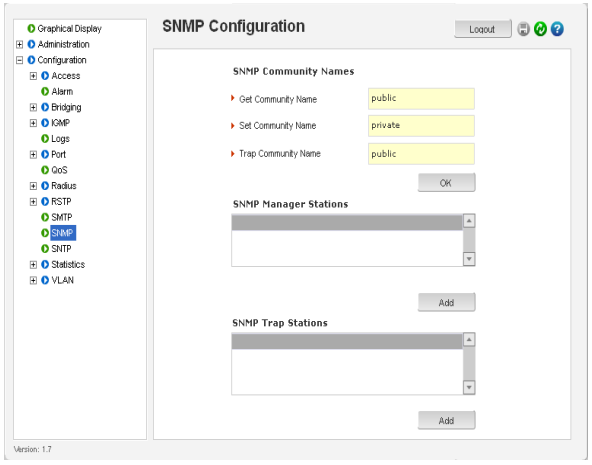
▷ Select the **Configuration > SNMP** menu item.



▷ Use the **Edit** button to change the SNMP community parameters.

▷ Use the **Add** buttons to add the management and trap receivers.

The following window illustrates changes to the SNMP community parameters. It is recommended to change the community strings from the default values of public and private to other values.



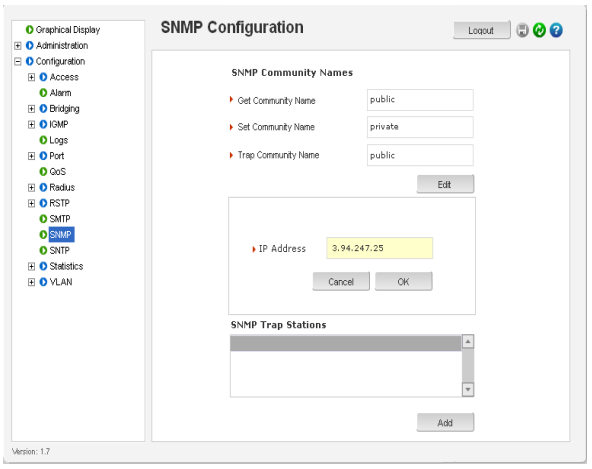
▷ When done changing the community strings, click **OK**.

Multiple managers can be added as shown below.

▷ When adding SNMP manager stations, click on the **Add** button on the SNMP menu screen.

▷ Make sure that each station can be pinged from the switch by using the **Configuration > Ping** menu.

▷ When done adding stations, click **OK**.

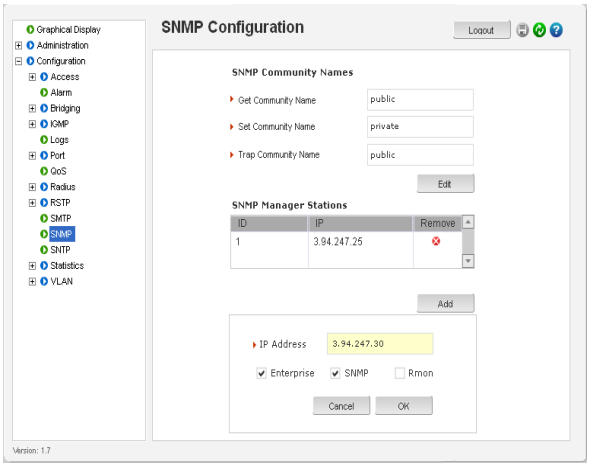


▷ When adding SNMP trap receivers, click on the Add button on the SNMP menu screen.

▷ Make sure that each station can be pinged from the switch by using the **Administration > Ping** menu.

▷ Determine which sorts of traps each station will receive, as shown above. If not sure, select all three types.

▷ **When done adding trap receivers, click OK.**



Note the different types of trap receivers added.

Stations can be deleted using the delete icon ( ). To change the stations characteristics or IP addresses, it is recommended to delete the station and add a new one.

▷ **After all changes are made, save the changes using the save icon ( ).**

16.4 Configuring RMON

16.4.1 Description

The switch supports RMON (Remote Monitoring) on all connected network segments. This allows for troubleshooting and optimizing your network. The MultiLink family of switches provides hardware-based RMON counters. The switch manager or a network management system can poll these counters periodically to collect the statistics in a format that compiles with the RMON MIB definition.

The following RMON groups are supported:

- **Ethernet statistics group** - maintains utilization and error statistics for the switch port being monitored.
- **History group** - gathers and stores periodic statistical samples from previous statistics group.
- **Alarm group** - allows a network administrator to define alarm thresholds for any MIB variable.
- **Log and event group** - allows a network administrator to define actions based on alarms. SNMP traps are generated when RMON alarms are triggered.

16.4.2 Commands

The following RMON communities, when defined, enable the specific RMON group as show above. The `rmon` command enter the RMON configuration mode to setup RMON groups and communities.

rmon

The `history` command defines the RMON history group and the community string associated with the group.

history *def-owner=<string> def-comm=<string>*

The `statistics` command defines the RMON statistics group and the community string associated with the group.

statistics *def-owner=<string>*
def-comm=<string>

The `alarm` command defines the RMON alarm group and the community string associated with the group.

alarm *def-owner=<string> def-comm=<string>*

The `event` command defines the RMON event group and the community string associated with the group.

event *def-owner=<string> def-comm=<string>*

The `show rom` command lists the specific RMON data as defined by the group type.

show rmon *<stats|hist|event|alarm>*

The following command sequence illustrates how to configure RMON groups.

ML2400(rmon)## `rmon`

ML2400(rmon)## `event def-owner=test def-comm=somestring`

```
RMON Event Default Owner is set
RMON Event Default Community is set
```

```
ML2400(rmon)## show rmon event
  RMON Event Default Owner     : test
  RMON Event Default Community : somestring
ML2400(rmon)## exit
ML2400#
```

Multilink ML2400

Ethernet Communications Switch

Chapter 17: Miscellaneous

17.1 Alarm Relays

17.1.1 Description

In a wiring closet, it would be helpful if there were a visual indication for faults on components on the network. Normally, these would be performed by LEDs. While the MultiLink switches have the necessary LEDs to provide the information needed, they also have provision for tripping or activating an external relay to electrically trigger any circuit desired. These could be an indicator light, a flashing strobe light, an audible alarm or other devices.

The MultiLink family of switches has a software (optional) controlled relay contact that can be use to report alarm conditions. The relay is held closed in normal circumstances and will go to the open position during alarm conditions.

Two types of alarm signals are defined in the alarm system.

- SUSTAINED
- MOMENTARY

The SUSTAINED mode is used to report a continuing error condition. The MOMENTARY mode is used to report a single event.

The following pre-defined events are currently supported on the ML2400 and the relay which can be triggered by software:

Table 17–1: Pre-defined conditions for the relay

Event ID	Description	Signal type
1	S-RING OPEN (see note below)	SUSTAINED
2	Cold Start	MOMENTARY
3	Warm Start	MOMENTARY
4	Link Up	MOMENTARY
5	Link Down	MOMENTARY
6	Authentication Failure	MOMENTARY
7	RMON Rising Alarm	MOMENTARY
8	RMON Falling Alarm	MOMENTARY
9	Intruder Alarm	MOMENTARY
10	Link Loss Learn Triggered	MOMENTARY
11	Broadcast Storm Detected	MOMENTARY
12	STP/RSTP Reconfigured	MOMENTARY
13	Power Supply A Failed	SUSTAINED
14	Power Supply B Failed	SUSTAINED

The S-RING OPEN event is not supported in the MultiLink ML2400 Ethernet Switch.

17.1.2 Configuring Alarm Relays through the Command Line Interface

To customize these capabilities, the ML2400 provides additional software capabilities and commands for configuring the alarm relays.

The `alarm` command enters the alarm configuration mode

alarm

The `add` command enables alarm action in response to the specified event ID.

add *event=<event-id|list|range|all>*

The `period` command sets the duration of relay action for the momentary type signal. This may be needed to adjust to the behavior of the circuit or relay. The time is in seconds, with a default of 3.

period *time=<1..10>*

The `del` command disables alarm action in response to the specified event ID.

del *event=<event-id|list|range|all>*

The `alarm` command globally enables or disables the alarm action.

alarm *<enable|disable>*

The `show alarm` command displays the current status of alarm system

show alarm

An example of setting up the external relays and alerts is shown below.

Alarm relays (continued)

```
ML2400(alarm)## add event=2

  Alarm Event(s) Added: 2

ML2400(alarm)## show alarm

  Alarm Events Configuration
    -------------------------
    Alarm Status: DISABLED
    Relay Closure Time Period: 5 Seconds

  EventId  Description                Mode
  ----------------------------------------
    1        S-RING OPEN                SUSTAINED
    2        Cold Start                 MOMENTARY
    3        Warm Start                 MOMENTARY
    4        Link Up                    MOMENTARY
    5        Link Down                  MOMENTARY
    6        Authentication Failure     MOMENTARY
    7        RMON Raising Alarm         MOMENTARY
    8        RMON Falling Alarm         MOMENTARY
    9        Intruder Alarm             MOMENTARY
    10       Link Loss Learn Triggered  MOMENTARY
    11       Broadcast Storm Detected   MOMENTARY
    12       STP/RSTP Reconfigured      MOMENTARY

ML2400(alarm)## alarm enable

  Alarm system Enabled

ML2400(alarm)## show alarm

  Alarm Events Configuration
    -------------------------
    Alarm Status: ENABLED
    Relay Closure Time Period: 5 Seconds

  EventId  Description                Mode
  ----------------------------------------
    1        S-RING OPEN                SUSTAINED
    2        Cold Start                 MOMENTARY
    3        Warm Start                 MOMENTARY
    4        Link Up                    MOMENTARY
    5        Link Down                  MOMENTARY
    6        Authentication Failure     MOMENTARY
    7        RMON Raising Alarm         MOMENTARY
    8        RMON Falling Alarm         MOMENTARY
    9        Intruder Alarm             MOMENTARY
    10       Link Loss Learn Triggered  MOMENTARY
    11       Broadcast Storm Detected   MOMENTARY
    12       STP/RSTP Reconfigured      MOMENTARY

ML2400(alarm)## alarm disable

  Alarm system Disabled

ML2400(alarm)## del event=1,3,5,7

  Alarm Event(s) Deleted: 1, 3, 5, 7
```

(continued on next page)

Example 17-1: Alarm relays

```
ML2400# alarm
ML2400(alarm)## add event=2

  Alarm Event(s) Added: 2

ML2400(alarm)## add event=1-5

  Event 2 is Already Enabled.
    Alarm Event(s) Added: 1, 3, 4, 5

ML2400(alarm)## add event=6,8

  Alarm Event(s) Added: 6, 8

ML2400(alarm)## add event=all

  Event 1 is Already Enabled.
    Event 2 is Already Enabled.
    Event 3 is Already Enabled.
    Event 4 is Already Enabled.
    Event 5 is Already Enabled.
    Event 6 is Already Enabled.
    Event 8 is Already Enabled.
    Alarm Event(s) Added: 7, 9, 10, 11, 12

ML2400(alarm)## del event=2

  Alarm Event(s) Deleted: 2

ML2400(alarm)## period time=5

  Relay closure Time Set.

ML2400(alarm)## show alarm

  Alarm Events Configuration
    -------------------------
    Alarm Status: DISABLED
    Relay Closure Time Period: 5 Seconds

  EventId  Description                Mode
  ----------------------------------------
    1        S-RING OPEN                SUSTAINED
    2        Cold Start                 NOT ENABLED
    3        Warm Start                 MOMENTARY
    4        Link Up                    MOMENTARY
    5        Link Down                  MOMENTARY
    6        Authentication Failure     MOMENTARY
    7        RMON Raising Alarm         MOMENTARY
    8        RMON Falling Alarm         MOMENTARY
    9        Intruder Alarm             MOMENTARY
    10       Link Loss Learn Triggered  MOMENTARY
    11       Broadcast Storm Detected   MOMENTARY
    12       STP/RSTP Reconfigured      MOMENTARY
```

(continued on next page)

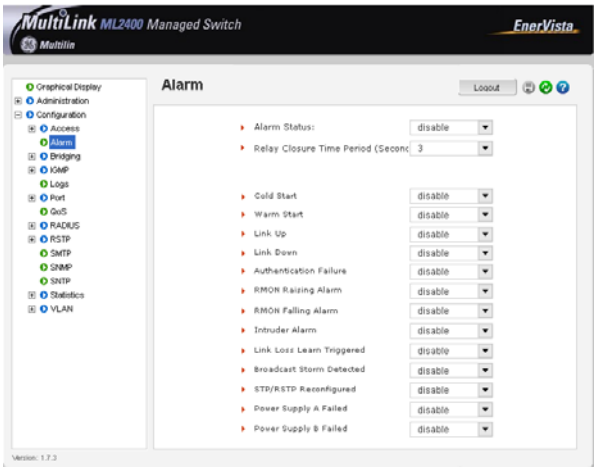
Alarm relays (continued)

```
ML2400(alarm)## show alarm

  Alarm Events Configuration
    -------------------------
    Alarm Status: DISABLED
    Relay Closure Time Period: 5 Seconds

  EventId  Description                Mode
  ----------------------------------------
    1        S-RING OPEN              NOT ENABLED
    2        Cold Start               MOMENTARY
    3        Warm Start               NOT ENABLED
    4        Link Up                  MOMENTARY
    5        Link Down                NOT ENABLED
    6        Authentication Failure   MOMENTARY
    7        RMON Raising Alarm       NOT ENABLED
    8        RMON Falling Alarm       MOMENTARY
    9        Intruder Alarm           MOMENTARY
    10       Link Loss Learn Triggered MOMENTARY
    11       Broadcast Storm Detected MOMENTARY
    12       STP/RSTP Reconfigured    MOMENTARY
ML2400(alarm)## exit
ML2400#
```

17.1.3 Configuring Alarm Relays with EnerVista Secure Web Management Software

To customize the alarm relays,

▷ Select the **Configuration > Alarms** menu item.



Each alarm can be enabled or disabled form the screen shown above. All alarms can be enabled or disabled using the Alarm Status drop down menu. Relay closure times can be set using the drop down menu.

▷ After changing the Alarm settings, save the configuration using the save icon ( ),

17.2 E-mail

17.2.1 Description

SMTP (RFC 821) is a TCP/IP protocol used in sending e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or Internet Message Access Protocol (IMAP) that lets the user save messages in a server mailbox and download them as needed from the server. In other words, users typically use a program that uses SMTP for sending e-mails (out going - e.g. replying to an e-mail message) and either POP3 or IMAP for receiving messages that have been arrived from the outside world. While SMTP (and its related protocols such as POP3, IMAP etc.) are useful transports for sending and receiving e-mails, it is extremely beneficial for a network administrator to receive e-mails in case of faults and alerts. The MultiLink family of switches can be setup to send and e-mail alert when a trap is generated.

If this capability is used, please ensure that SPAM filters and other filters are not set to delete these e-mails.

GE Multilin recommends that a rule be setup on the mail server so that all e-mails indicating SNMP faults are automatically stored in a folder or redirected to the necessary administrators.

The SNMP alerts can be configured using the MultiLink Switch Software for the following:

- Send e-mail alert according to the configuration rules when a specific event category happens.
- Send e-mail alert according to the configuration rules when a specific trap SNMP trap category happens.
- Provide configuration and customization commands for users to specify SMTP server to connect to, TCP ports, user recipients and filters.
- The SMTP alerts provide the following capabilities:
- SMTP alerts can be enabled or disabled globally.
- User can defined a global default SMTP server identified by its IP address, TCP port and retry count.
- User can add up to five SMTP alert recipients. Each recipient is identified by an ID and e-mail address. The e-mail address needs to be a valid address and can be an alias setup for distribution to a larger audience.
- Filters are provided for each recipient to allow only certain categories of traps and events be sent by e-mail.
- Each recipient can have its own SMTP server and TCP port number, if this is not defined on a certain recipient, the default SMTP server and TCP port number is used.

17.2.2 Commands

The `smtp` command configures the SNMP alerts to be sent via e-mail.

smtp
smtp *<enable|disable>*

The `show smtp` command displays the current SMTP global settings and recipients displays the currently configured recipients of e-mail alerts.

show smtp *<config|recipients>*

The `add` command adds a specific `id`, where `id` represents the recipient identification and ranges from 1 to 5. The software allows a maximum of 5 recipients

add *id=<1-5> email=<email-addr> [traps=<all|none|S|R|E>] [events=<all|none|I|A|C|F|D>] [ip=<ip-addr>] [port=<1-65535>] [domain=<domain>]*

The `add` command has the following additional parameters:

- The `email` parameter is the e-mail address of the recipient.
- The optional `traps` parameter represents the trap filter. If value is all, all traps of any type will be sent to this recipient. If value is none, no traps are sent to this recipient. Value can also be a combination of 'S' (SNMP), 'R' (RMON) and 'E' (enterprise). For example, `trap=SR` means that SNMP and RMON traps will be sent via e-mail to the recipient. If this option is not defined, the recipient will have a default value of "all".
- The optional `events` parameter is the event filter. Value can be "all" - all event severity types will be sent to recipient, "none" - no event will be sent to recipient or a combination of 'I' (informational), 'A' (activity), 'C' (critical), 'F' (fatal) and 'D' (debug). With "`event=ACF`" implies that events of severity types activity, critical and fatal will be sent to recipients by e-mail. If this option is not defined, a value of "all" is taken.
- The optional `ip` parameter represents the SMTP server IP address. This is the SMTP server to connect to for this particular user. If this option is not defined, the global/ default SMTP server is used.
- The optional `port` parameter specifies the TCP port of the SMTP server. If this is not defined, the global default TCP port is used.

The `optional domain` parameter specifies the domain name of the SMTP server. If this is not defined, the global default domain name is used.

The `delete` command deletes the specific `id` specified. The deleted `id` no longer receives the traps via e-mail. The `id` is added using the `add` command

delete *id=<1-5>*

The `sendmail` command customizes (and also sends a test e-mail to check SMTP settings) the e-mail delivered by specifying the e-mail subject field, server address, to field and the body of the text. See the example in this section for details.

sendmail *server=<ip-addr> to=<email-addr> from=<email-addr> subject=<string> body=<string>*

The `server` command configures the global SMTP server settings.

server *ip=<ip-addr> [port=<1-65535>] [retry=<0-3>] [domain=<domain>]*

For this command, `ip` represents the SMTP server IP address, `port` the TCP port to be used for SMTP communications (default is 25), and `retry` specifies how many times to retry if an error occurs when sending e-mail (from 0 to 3 with default of 0).

The `optional domain` parameter specifies the domain name of the SMTP server.

17.2.3 Example

The following example shows how to set SMTP to receive SNMP trap information via e-mail.

E-mail alerts can be forwarded to be received by other devices such as cellphones and pages. Most interfaces to SMTP are already provided by the service provider.

Example 17-2: Configuring SMTP to receive SNMP trap information via e-mail

```
ML2400#smtp
ML2400(smtp)##server ip=3.94.210.25 port=25 retry=3 domain=ge.com
  Successfully set global SMTP server configuration
ML2400(smtp)##show smtp config
         SMTP Global Configuration
  ========================================
  Status             :  Disabled
  SMTP Server Host   :  3.94.210.25
  SMTP Server Domain :  ge.com
  SMTP Server Port   :  25
  Retry Count        :  3
ML2400(smtp)##add id=1 email=jsmith@ge.com traps=s events=CF
  Recipient successfully added
ML2400(smtp)##add id=2 email=xyz@abc.com traps=all events=all ip=3.30.154.28 port=25
  domain=abc.com
  Recipient successfully added
ML2400(smtp)##show smtp recipients
ID E-mail Address  SMTP Server    From Domain    Port  Traps Events
=================================================================
1  jsmith@ge.com  3.94.210.25      ge.com         25     S      FC
2  xyz@abc.com    3.30.154.28      abc.com        25    All    All
3  --               --              --           --     --     --
4  --               --              --           --     --     --
5  --               --              --           --     --     --
ML2400(smtp)##delete id=2
  Recipient successfully deleted
ML2400(smtp)##show smtp recipients
ML2400(smtp)##show smtp recipients
ID E-mail Address  SMTP Server    From Domain    Port  Traps Events
=================================================================
1  jsmith@ge.com  3.94.210.25      ge.com         25     S     FC
2  --               --              --           --     --    --
3  --               --              --           --     --    --
4  --               --              --           --     --    --
5  --               --              --           --     --    --
```

17.3 Statistics

17.3.1 Viewing Port Statistics with EnerVista Secure Web Management Software

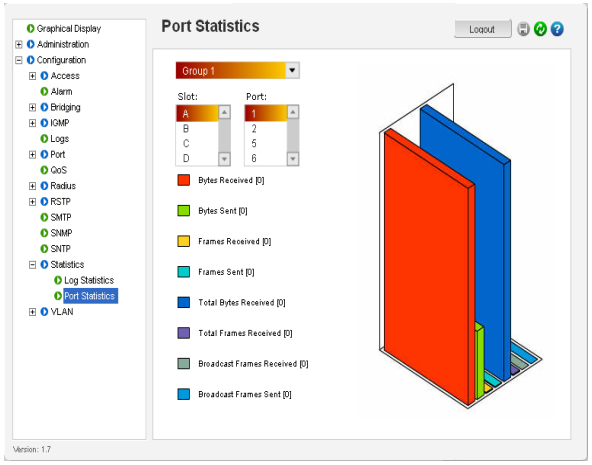
The EnerVista Secure Web Management Software allows for the display of several statistics in a graphical format. These are described below.

To view statistics,

▷ Select the **Configuration > Statistics** menu item.

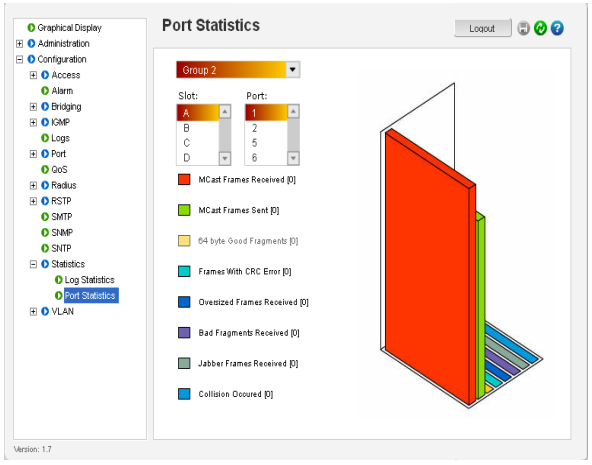
To view port-specific statistics,

▷ Select the **Configuration > Statistics > Port Statistics** menu item.

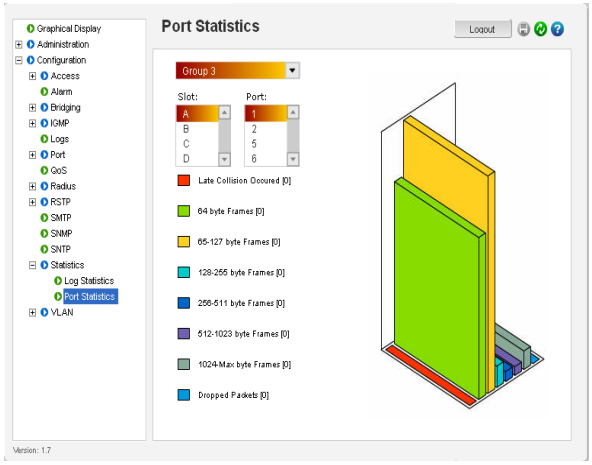


Each port can be viewed by clicking on the back or forward buttons. Each group represents different statistics.

The following figure displays the port statistics for group 2.



The following figure displays the port statistics for group 3.



17.4 Serial Connectivity

17.4.1 Description

When using the serial connectivity with applications such as HyperTerminal, it may be necessary to optimize the character delays so that the FIFO buffer used in the MultiLink switches is not overrun. The important parameters to set for any serial connectivity software is to set the line delay to be 500 ms and the character delay to be 50 ms. For example, using HyperTerminal this can be set under **File > Properties**. When the **Properties** window is open, click on the **ASCII Setup** button and in the **Line Delay** entry box enter in 500 and in the **Character Delay** entry box enter in 50 as shown below.

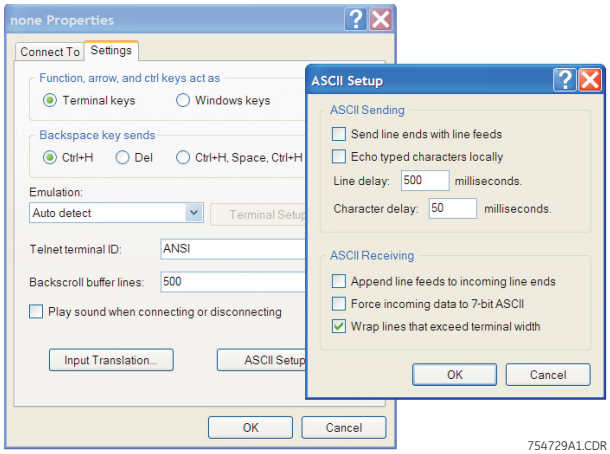


FIGURE 17–1: Optimizing serial connection in HyperTerminal

17.5 History

17.5.1 Commands

The commands below may be useful in repeating commands and obtaining history information.

The `!!` command repeats the last command.

!!

The `!1`, `!2`,..., `!n` commands repeat the *n*th command (as indicated by a show history).

!<n>

The `show history` command displays the last 25 executed commands. If less than 25 commands were executed, only those commands executed are shown.

show history

The history is cleared if the user logs out or if the switch times out. The history count restarts when the user logs in.

The `show version` command displays the current software version.

show version

17.6 Ping

17.6.1 Ping through the Command Line Interface

The `ping` command can be used to test connectivity to other devices as well as checking to see if the IP address is setup correctly. The command syntax is:

ping *<ipaddress> [count=<1-999>] [timeout=<1-256>]*

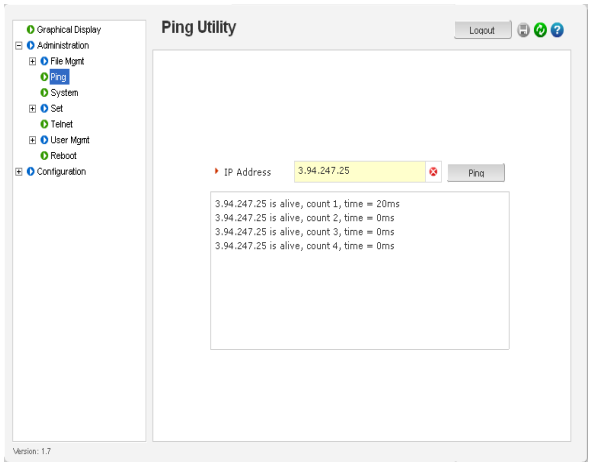
For example:

```
ML2400# ping 3.94.248.61
3.94.248.61 is alive, count 1, time = 40ms
ML2400# ping 3.94.248.61 count=3
3.94.248.61 is alive, count 1, time = 20ms
  3.94.248.61 is alive, count 2, time = 20ms
  3.94.248.61 is alive, count 3, time = 40ms
ML2400#
```

Many devices do not respond to `ping` or block `ping` commands. Make sure that the target device responds or the network allows the ping packets to propagate.

17.6.2 Ping through EnerVista Secure Web Management Software

The `ping` command can be used from EnerVista Secure Web Management Software to test connectivity to other devices as well as checking to see if the IP address is correct. Select the **Administration > Ping** menu item to use ping.



As mentioned earlier, many devices do not respond to `ping` commands. Make sure that the target device responds or the network allows ping packets to propagate.

17.7 Prompt

17.7.1 Changing the Command Line Prompt

Setting a meaningful host prompt can be useful when a network administrator is managing multiple switches and has multiple telnet or console sessions. To facilitate this, the ML2400 allows administrators to define custom prompts. The command to set a prompt is:

set prompt *<prompt string>*

The length of the prompt is limited to 60 characters.

There are predefined variables that can be used to set the prompt. These are:

- $n: system name
- $c: system contact
- $l: system location
- $i: system IP address
- $m: system MAC address
- $v: version
- $$: the "$" (dollar sign) character
- $r: new line
- $b: space

A few examples on how the system prompt can be setup are shown below.

```
ML2400# snmp
ML2400(snmp)## setvar sysname=Core
  System variable(s) set successfully
ML2400(snmp)## exit
ML2400# set prompt $n
Core# set prompt $n$b$i
Core 192.168.5.5# set prompt $n$b$i$b
Core 192.168.5.5 # snmp
Core 192.168.5.5 (snmp)## setvar sysname=ML2400
  System variable(s) set successfully
Core 192.168.5.5 (snmp)## exit
Core 192.168.5.5 # set prompt $b$b$i$b
192.168.5.5 # set prompt $n$b$i$b
ML2400 192.168.5.5 #
ML2400 192.168.5.5 # set prompt Some$bthing$i
Some thing192.168.5.5# set prompt Some$bthing$b$i
Some thing 192.168.5.5#
```

17.8 System Events

17.8.1 Description

The event log records operating events as single-line entries listed in chronological order, and are a useful tool for isolating problems. Each event log entry is composed of four fields as shown below:

- **Severity** field: Indicates one of the following
- I (Information) indicates routine events; A (Activity) indicates activity on the switch; D (Debug) is reserved for GE Multilin; C (Critical) indicates that a severe switch error has occurred; and F (Fatal). indicates that a service has behaved unexpectedly.
- **Date** field: the date in mm/dd/yy format (as per configured) that the entry was placed in the log.
- **Time** field: is the time in hh:mm:ss format (as per configured) that the entry was placed in the log.
- **Description** field: is a brief description of the event.

The event log holds up to 1000 lines in chronological order, from the oldest to the newest. Each line consists of one complete event message. Once the log has received 1000 entries, it discards the current oldest line (with information level severity only) each time a new line is received. The event log window contains 22 log entry lines and can be positioned to any location in the log.

17.8.2 Command Line Interface Example

The following example illustrates a typical event log.

Example 17-3: Typical system event log

```
ML2400# show log
  S   DATE         TIME           Log Description
    --  ----------   ------------   ------------------------------------------------
    I   03-02-2005    5:14:43 P.M   SYSMGR:System Subnet Mask changed
    I   01-01-2001   12:00:00 A.M   SYSMGR:successfully registered with DB Manager
    I   01-01-2001   12:00:00 A.M   SYSMGR:successfully read from DB
    A   01-01-2001   12:00:00 A.M   VLAN:Vlan type set to Port VLAN
    I   01-01-2001   12:00:00 A.M   SYSMGR:system was reset by user using CLI command
    I   01-01-2001   12:00:00 A.M   SNTP:Date/Time set to 01-01-2001 12:00AM
    I   01-01-2001   12:00:00 A.M   SNTP:Client started
    I   03-03-2005    4:32:48 A.M   SNTP:Date and Time updated from SNTP server
    I   03-03-2005    9:31:59 A.M   TELNET:Telnet Session Started
    I   03-03-2005    9:32:04 A.M   CLI:manager console login|
    A   03-03-2005    9:32:11 A.M   IGMP:IGMP Snooping is enabled
    A   03-03-2005    9:35:40 A.M   IGMP:IGMP Snooping is disabled
    A   03-03-2005    9:41:46 A.M   IGMP:IGMP Snooping is enabled
ML2400#
```

Event logs can be exported to a ftp or a tftp server on the network for further analysis. The CLI command is used to facilitate the export of the event log

exportlog *mode=<serial|tftp|ftp> <ipaddress> file=<name> doctype=<raw|html>*

Where `mode` is the mode of transfer, `ipaddress` is the IP address of the ftp or TFTP server, `file` is the filename, and `doctype` indicates the log is saved as a text file (raw) or as an HTML file.

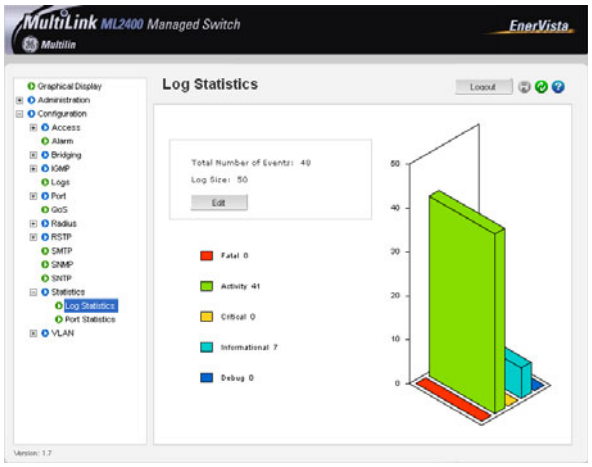
Please ensure the proper extension is used for the `file` argument (for example, "html" for an HTML file).

```
ML2400# exportlog mode=tftp 192.168.5.2 file=eventlog doctype=html
Do you wish to export the event logs? [ 'Y' or 'N'] Y
Successfully uploaded the event log file.
ML2400# exportlog mode=tftp 192.168.5.2 file=eventlog.txt
  doctype=raw
Do you wish to export the event logs? [ 'Y' or 'N'] Y
Successfully uploaded the event log file.
```

17.8.3 EnerVista Example

The EnerVista Secure Web Management Software provides and overview of the type of Logs by reviewing the statistics. Each specific log can be viewed by viewing the logs menu. To view the log statistics,

▷ select the **Configuration > Statistics > Log Statistics** menu item.

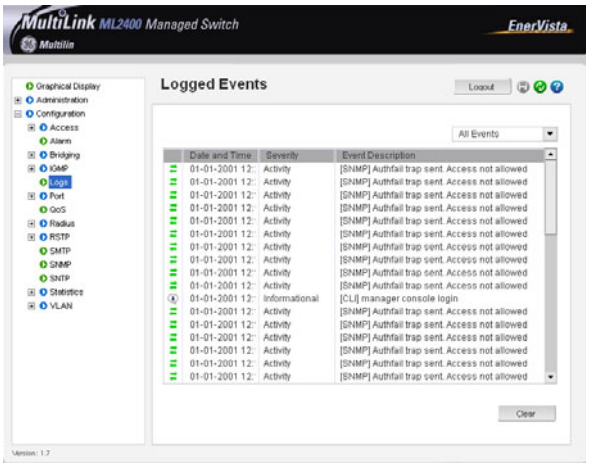


The **Log Statistics** window displays the logged events received – most logs are typically informational and activity.

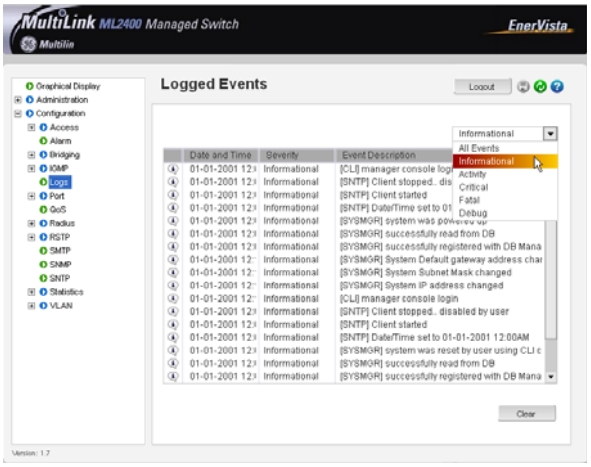
The log buffer size can be controlled through this menu.

For viewing each specific log,

▷ Select the **Configuration > Logs** menu item.



Each specific type of log can be viewed by using the drop down menu as shown below. In this example only informational logs are displayed.



The Clear button clears all the logs. To prevent accidental erasures, you will be prompted again if the logs should be deleted.

The Event Log records operating events as single-line entries listed in chronological order. For details on event log records, refer to *Description* on page 17–15.

17.9 Command Reference

17.9.1 Main Commands

The main commands can be categorized as show commands, set commands, and context-less commands. The show commands are listed below.

- `show active-snmp`: displays currently active SNMP support
- `show active-stp`: displays currently active STP
- `show active-vlan`: displays currently active VLAN
- `show address-table`: displays address table parameters
- `show age`: displays the address table age limit
- `show arp`: displays the arp details
- `show bootmode`: displays the current bootmode value
- `show broadcast-protect`: displays broadcast storm protection parameters
- `show config`: displays the saved configuration as a whole or by module
- `show console`: displays console serial link settings
- `show date`: displays system date
- `show daylight`: displays the configured daylight savings settings
- `show gateway`: displays the gateway of the system
- `show gvrp`: displays the GVRP parameters
- `show host`: displays the host table for FTP users
- `show igmp`: displays the IGMP parameters
- `show interfaces`: display the interface information
- `show ip`: displays the system IP address
- `show ip-access`: displays the IP address access list
- `show ipconfig`: displays the IP configuration
- `show lacp`
- `show lll`: displays the Link-Loss-Learn parameters
- `show log`: displays log information
- `show logsize`: displays the current event log size
- `show mac`: displays the system MAC address
- `show modbus`: displays Modbus settings
- `show modules`: displays the module information
- `show port`: displays the port information
- `show port-mirror`: displays the port mirroring parameters
- `show port-security`: displays the port security configuration parameters
- `show power`: displays condition of power supplies, in redundant power supply switches only
- `show qos`: displays the QOS settings
- `show rmon`: displays the rmon configuration parameters
- `show setup`: displays the setup parameters of the system

- `show smtp`: displays e-mail (SMTP) alert information
- `show snmp`: displays information related to SNMP
- `show sntp`: displays the configured SNTP servers details
- `show stats`: displays the port statistics
- `show stp`: displays Spanning Tree Bridge parameters
- `show subnet`: displays the Subnet Mask of the system
- `show ssl`
- `show sysconfig`: displays system configurable parameters
- `show syscontact`: displays the current system contact
- `show syslocation`: displays the current system location
- `show sysname`: displays the current system name
- `show time`: displays the system time
- `show timeout`: displays the system inactivity time out
- `show timezone`: displays the configured time zone of the device
- `show uptime`: displays up time of the system
- `show users`: displays all configured users
- `show version`: displays current version of the software
- `show vlan`: displays the VLAN parameters of a specified type
- `show web`

The set commands are listed below.

- `set bootmode`
- `set date year`
- `set daylight country`
- `set prompt`
- `set logsize`
- `set password`: sets the current user password
- `set snmp`
- `set stp`
- `set time`
- `set timeformat`
- `set timeout`: sets the system inactivity time out
- `set timezone`
- `set vlan`: sets the VLAN type

The context-less commands are listed below.

- `clear`: clears the event log, command history, or screen
- `climode`: to set the interactive CLI mode
- `enable`: allows to login as another user
- `help`
- `host`: to generate the host table for FTP users
- `more`: to set more pipe in screen outputs

- save
- whoami: display the user information
- reboot
- authorize
- degrade
- exportlog mode
- ftp
- help
- ipconfig
- kill
- kill session id
- logout: logs out from the current user
- ping: to send the ping requests
- tftp
- telnet: connects to the remote system through telnet
- terminal: to set the terminal size
- xmodem

17.9.2 Configuration commands

The access commands are shown below.

- allow: allows the IP address
- deny: denies the IP address
- dhcp: enables or disables the DHCP
- modbus: enables or disables access to Modbus map
- remove
- removeall
- snmp: enables or disables SNMP
- ssl
- telnet
- web

The alarm commands are shown below. Refer to *Alarm Relays* on page 17–1 for details on using these commands.

- add
- alarm
- del
- period

The authorization commands are shown below.

- auth
- authserver
- backend

- clear-stats
- portaccess
- reauth
- setport
- show-port
- show-stats
- trigger-reauth

The device commands are shown below.

- device
- backpressure
- broadcast-protect: enables or disables broadcast storm protection globally
- flowcontrol
- rate-threshold: sets the broadcast rate threshold (frames/sec)
- setage: sets the mgtagetime
- setport: sets the port configuration

The VLAN registration over GARP (GVRP) commands are shown below. Refer to *VLAN Registration over GARP* on page 11–1 for details.

- gvrp
- help gvrp: configures GVRP parameters for dynamic VLAN
- set-forbid: sets forbidden ports for a tag-based VLAN
- show-ports: show ports current GVRP state
- show-forbid: show forbidden ports for tag-based VLAN
- set-ports: set GVRP port state usage
- show-vlan: shows dynamic/static tag-based VLANs
- static: convert dynamic VLAN to static VLAN

The IGMP commands are shown below. Refer to *IGMP* on page 15–1 for additional details.

- mcast
- set-leave: enables or disables IGMP immediate leave status
- set-port: sets the port mode
- set-qi: sets the query interval (60 to 127) for router ports
- set-qri
- set-querier: enables or disables switch as querier
- show-group: displays IGMP group list
- show-port: displays IGMP port mode
- show-router: displays IGMP router list

The Link Aggregation Control Protocol (LACP) commands are shown below.

- lacp
- add port
- del port
- edit port

The port mirroring commands are shown below. Refer to *Port Mirroring* on page 9–1 for additional details.

- `help port-mirror`
- `prtmr`: enables/disables port mirroring functionality
- `setport`: defines the port mirroring ports

The port security commands are shown below. Refer to *Securing Access* on page 6–1 for additional details.

- `action`: sets the action type of secured port
- `allow`: allows MAC addressing per port
- `help port-security`
- `learn`: enables/disables security for a single port or group of ports
- `ps`: enables/disables security in system
- `remove`: removes MAC addressing per port
- `signal`: sets the signal type of the secured port

The quality of service (QoS) commands are shown below. Refer to *QoS Overview* on page 14–1 for additional details.

- `help qos`
- `setqos`: configures QOS configuration usage
- `set-untag`
- `set-weight`: sets the port priority weights for all the ports in all the device
- `show-portweight`: displays the current port weight priority

The remote monitoring (RMON) commands are shown below. Refer to *Configuring RMON* on page 16–13 for additional details.

- `alarm`: sets the owner for the alarm group
- `event`: sets the owner for the event group
- `help rmon`
- `history`: sets the owner for the history group
- `statistics`: sets the owner for the statistics group

The Rapid Spanning Tree Protocol (RSTP) commands are shown below. Refer to *Rapid Spanning Tree Protocol* on page 13–1 for additional details.

- `cost`: sets the path cost of ports
- `forceversion`: set the force version of STP
- `help rstp`
- `lll`
- `port`: sets the RSTP administration status of ports
- `priority`: changes the priority of ports or bridge
- `rstp`: changes the RSTP administrative status of the bridge
- `show-forceversion`: shows the current force version of RSTP
- `show-mode`: shows the port mode status
- `show-timers`: shows the bridge time parameters
- `timers`: changes the bridge time parameters

The Simple Mail Transfer Protocol (SMTP) commands for e-mail are shown below. Refer to *E-mail* on page 17–6 for additional details.

- `add`: adds a recipient
- `delete`: deletes a recipient
- `help smtp`
- `sendmail`: sends e-mail
- `server`: sets the global SMTP server configuration
- `smtp`: enables/disables SMTP e-mail alert

The Simple Network Management Protocol (SNMP) commands are shown below. Refer to *SNMP* on page 16–1 for additional details.

- `authentraps`: enable/disables the authentication traps
- `community`: configures SNMP community names
- `help snmp`
- `mgrip`: adds or deletes the SNMP manager IP
- `setvar`: configures system name, contact, or location
- `traps`: adds or deletes a trap receiver

The Simple Network Time Protocol (SNTP) commands are shown below. Refer to *Network Time* on page 5–10 for additional details.

- `delete`: deletes the SNTP server from SNTP server database
- `help sntp`
- `setsntp`: adds SNTP server into the SNTP server database
- `sntp`: configures parameters for SNTP system
- `sync`: sets the interval for synchronization time with an NTP server

The Spanning Tree Protocol (STP) commands are shown below. Refer to *Spanning Tree Protocol (STP)* on page 12–1 for additional details.

- `cost`
- `lll`
- `port`
- `priority`
- `s-ring`
- `stp`
- `timers`

The user commands are shown below. Refer to the *User Management* on page 1–14 for additional details.

- `add`: adds a new user
- `chlevel`: changes the user access permissions
- `delete`: deletes an existing user
- `help user`
- `passwd`: change the user password
- `tacplus`
- `tacserver`

- useraccess

The VLAN commands are shown below. Refer to *VLAN* on page 10–1 for additional details.

- add
- delete
- edit
- save
- set-egress
- set-ingress
- set-port
- show-egress
- show-ingress
- show-port
- start
- stop
- vlan

Multilink ML2400

Ethernet Communications Switch

Chapter 18: Modbus Protocol

18.1 Modbus Configuration

18.1.1 Overview

Modicon programmable controllers as well as other PLCs can communicate with each other and other devices over a variety of networks. The common language used by all Modicon controllers is the Modbus protocol. This protocol defines a message structure that controllers recognize and use regardless of the networks over which they communicate. It describes the process a controller uses to request access to another device, how it will respond to requests from the other devices, and how errors will be detected and reported. It establishes a common format for the layout and contents of message fields. The Modbus protocol thus operates at the layer 7 of the OSI 7 layer stack. Additional information on Modbus can be found at http://www.modbus.org and other related sites.

RFC 1122 Requirements for Internet Hosts - Communication Layers defines how Modbus packets can be carried over a TCP/IP transport and how Modicon controllers or other PLC devices can communicate over a TCP/IP network. To facilitate this communications, the GE Multilink switches allow Modbus connectivity.

As per this RFC, Modbus communications take place on TCP port 502. Please make sure the network security devices do not block port 502. If port 502 is blocked, which is the normal case with many firewall and other security devices, the communications between two Modbus devices over a TCP/IP network will not succeed.

18.1.2 Command Line Interface Settings

The following command-line interface settings are available:

modbus *<enable|disable>*
modbus *port=<port|default>*
modbus *device=<device|default>*
show modbus

The commands enable the Modbus protocol and set the relevant Modbus slave address and communication port values.

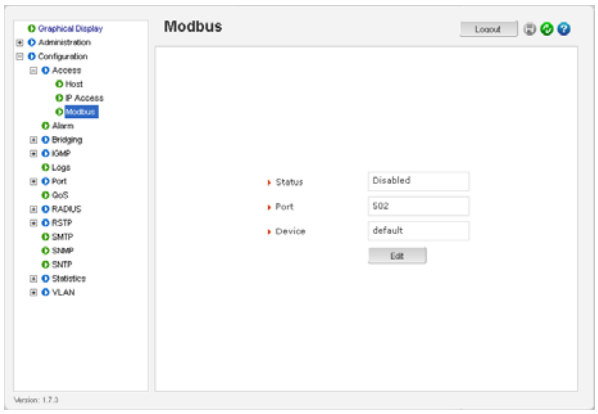
For example,

```
ML2400# show ipconfig

  IP Address:      192.168.1.5
  Subnet Mask:     255.255.255.0
  Default Gateway: 192.168.1.10

ML2400# show modbus

  Access to Modbus disabaled
  Modbus is Using Port: 502
  Modbus is Using Device: 5

ML2400# access

ML2400(access)## modbus enable

  Enabling Access to Modbus

ML2400(access)## show modbus

  Access to Modbus enabled
  Modbus is Using Port: 502
  Modbus is Using Device: 5

ML2400(access)## modbus port=602

  Modbus Port is set

ML2400(access)## show modbus

  Access to Modbus enabled
  Modbus is Using Port: 602
  Modbus is Using Device: 5

ML2400(access)## modbus port=default

  Modbus Port Set to Default

ML2400(access)## show modbus

  Access to Modbus enabled
  Modbus is Using Port :502
  Modbus is Using Device :5
```

18.1.3 EnerVista Settings

To modify the Modbus settings through EnerVista Secure Web Management software,

▷ Select the **Configuration > Access > Modbus** menu item.



18.2 Memory Mapping

18.2.1 Modbus Memory Map

The Modbus memory map is shown below. Refer to *Format Codes* on page 18–36 for details on the items in the format column.

Table 18–1: Modbus memory map (Sheet 1 of 33)

Address	Description	Range	Step	Format	Default
0000	System name (12 registers)	-	-	String	Varies
000C	System contact (12 registers)	-	-	String	multilin.tech @ge.com
0018	System location (12 registers)	-	-	String	Markham, Ontario
0024	Software version (6 registers)	-	-	String	Varies
002A	IP address (byte 0)	1 to 254	1	F1	0
002B	IP address (byte 1)	1 to 254	1	F1	0
002C	IP address (byte 2)	1 to 254	1	F1	0
002D	IP address (byte 3)	1 to 254	1	F1	0
002E	Netmask (byte 0)	1 to 254	1	F1	0
002F	Netmask (byte 1)	1 to 254	1	F1	0
0030	Netmask (byte 2)	1 to 254	1	F1	0
0031	Netmask (byte 3)	1 to 254	1	F1	0
0032	Gateway (byte 0)	1 to 254	1	F1	0
0033	Gateway (byte 1)	1 to 254	1	F1	0
0034	Gateway (byte 2)	1 to 254	1	F1	0
0035	Gateway (byte 3)	1 to 254	1	F1	0
0036	MAC address (3 registers)	-	-	String	Varies
0039	Order code (16 registers)	-	-	String	Varies
0049	Power alarm 1	0 to 1	1	F2	0
004A	Power alarm 2	0 to 1	1	F2	0
004B	Stp State	0 to 1	1	F3	0
004C	Number of ports	1 to 32	1	F1	Varies
004E	Port present map	-	-	Bitmap	Varies
0050	Port link map	-	-	Bitmap	0
0052	Port stp state map	-	-	Bitmap	0
0054	Port activity map	-	-	Bitmap	0
0056	Port 1 type	0 to 6	1	F4	Varies
0057	Port 2 type	0 to 6	1	F4	Varies
0058	Port 3 type	0 to 6	1	F4	Varies
0059	Port 4 type	0 to 6	1	F4	Varies
005A	Port 5 type	0 to 6	1	F4	Varies
005B	Port 6 type	0 to 6	1	F4	Varies
005C	Port 7 type	0 to 6	1	F4	Varies
005D	Port 8 type	0 to 6	1	F4	Varies
005E	Port 9 type	0 to 6	1	F4	Varies
005F	Port 10 type	0 to 6	1	F4	Varies
0060	Port 11 type	0 to 6	1	F4	Varies
0061	Port 12 type	0 to 6	1	F4	Varies

Table 18–1: Modbus memory map (Sheet 2 of 33)

Address	Description	Range	Step	Format	Default
0062	Port 13 type	0 to 6	1	F4	Varies
0063	Port 14 type	0 to 6	1	F4	Varies
0064	Port 15 type	0 to 6	1	F4	Varies
0065	Port 16 type	0 to 6	1	F4	Varies
0066	Port 17 type	0 to 6	1	F4	Varies
0067	Port 18 type	0 to 6	1	F4	Varies
0068	Port 19 type	0 to 6	1	F4	Varies
0069	Port 20 type	0 to 6	1	F4	Varies
006A	Port 21 type	0 to 6	1	F4	Varies
006B	Port 22 type	0 to 6	1	F4	Varies
006C	Port 23 type	0 to 6	1	F4	Varies
006D	Port 24 type	0 to 6	1	F4	Varies
006E	Port 25 type	0 to 6	1	F4	Varies
006F	Port 26 type	0 to 6	1	F4	Varies
0070	Port 27 type	0 to 6	1	F4	Varies
0071	Port 28 type	0 to 6	1	F4	Varies
0072	Port 29 type	0 to 6	1	F4	Varies
0073	Port 30 type	0 to 6	1	F4	Varies
0074	Port 31 type	0 to 6	1	F4	Varies
0075	Port 32 type	0 to 6	1	F4	Varies
0076	Port 1 link status	0 to 1	1	F3	0
0077	Port 2 link status	0 to 1	1	F3	0
0078	Port 3 link status	0 to 1	1	F3	0
0079	Port 4 link status	0 to 1	1	F3	0
007A	Port 5 link status	0 to 1	1	F3	0
007B	Port 6 link status	0 to 1	1	F3	0
007C	Port 7 link status	0 to 1	1	F3	0
007D	Port 8 link status	0 to 1	1	F3	0
007E	Port 9 link status	0 to 1	1	F3	0
007F	Port 10 link status	0 to 1	1	F3	0
0080	Port 11 link status	0 to 1	1	F3	0
0081	Port 12 link status	0 to 1	1	F3	0
0082	Port 13 link status	0 to 1	1	F3	0
0083	Port 14 link status	0 to 1	1	F3	0
0084	Port 15 link status	0 to 1	1	F3	0
0085	Port 16 link status	0 to 1	1	F3	0
0086	Port 17 link status	0 to 1	1	F3	0
0087	Port 18 link status	0 to 1	1	F3	0
0088	Port 19 link status	0 to 1	1	F3	0
0089	Port 20 link status	0 to 1	1	F3	0
008A	Port 21 link status	0 to 1	1	F3	0
008B	Port 22 link status	0 to 1	1	F3	0
008C	Port 23 link status	0 to 1	1	F3	0
008D	Port 24 link status	0 to 1	1	F3	0
008E	Port 25 link status	0 to 1	1	F3	0
008F	Port 26 link status	0 to 1	1	F3	0

Table 18–1: Modbus memory map (Sheet 3 of 33)

Address	Description	Range	Step	Format	Default
0090	Port 27 link status	0 to 1	1	F3	0
0091	Port 28 link status	0 to 1	1	F3	0
0092	Port 29 link status	0 to 1	1	F3	0
0093	Port 30 link status	0 to 1	1	F3	0
0094	Port 31 link status	0 to 1	1	F3	0
0095	Port 32 link status	0 to 1	1	F3	0
0096	Port 1 STP state	0 to 1	1	F3	0
0097	Port 2 STP state	0 to 1	1	F3	0
0098	Port 3 STP state	0 to 1	1	F3	0
0099	Port 4 STP state	0 to 1	1	F3	0
009A	Port 5 STP state	0 to 1	1	F3	0
009B	Port 6 STP state	0 to 1	1	F3	0
009C	Port 7 STP state	0 to 1	1	F3	0
009D	Port 8 STP state	0 to 1	1	F3	0
009E	Port 9 STP state	0 to 1	1	F3	0
009F	Port 10 STP state	0 to 1	1	F3	0
00A0	Port 11 STP state	0 to 1	1	F3	0
00A1	Port 12 STP state	0 to 1	1	F3	0
00A2	Port 13 STP state	0 to 1	1	F3	0
00A3	Port 14 STP state	0 to 1	1	F3	0
00A4	Port 15 STP state	0 to 1	1	F3	0
00A5	Port 16 STP state	0 to 1	1	F3	0
00A6	Port 17 STP state	0 to 1	1	F3	0
00A7	Port 18 STP state	0 to 1	1	F3	0
00A8	Port 19 STP state	0 to 1	1	F3	0
00A9	Port 20 STP state	0 to 1	1	F3	0
00AA	Port 21 STP state	0 to 1	1	F3	0
00AB	Port 22 STP state	0 to 1	1	F3	0
00AC	Port 23 STP state	0 to 1	1	F3	0
00AD	Port 24 STP state	0 to 1	1	F3	0
00AE	Port 25 STP state	0 to 1	1	F3	0
00AF	Port 26 STP state	0 to 1	1	F3	0
00B0	Port 27 STP state	0 to 1	1	F3	0
00B1	Port 28 STP state	0 to 1	1	F3	0
00B2	Port 29 STP state	0 to 1	1	F3	0
00B3	Port 30 STP state	0 to 1	1	F3	0
00B4	Port 31 STP state	0 to 1	1	F3	0
00B5	Port 32 STP state	0 to 1	1	F3	0
00B6	Port 1 activity	0 to 1	1	F3	0
00B7	Port 2 activity	0 to 1	1	F3	0
00B8	Port 3 activity	0 to 1	1	F3	0
00B9	Port 4 activity	0 to 1	1	F3	0
00BA	Port 5 activity	0 to 1	1	F3	0
00BB	Port 6 activity	0 to 1	1	F3	0
00BC	Port 7 activity	0 to 1	1	F3	0
00BD	Port 8 activity	0 to 1	1	F3	0

Table 18–1: Modbus memory map (Sheet 4 of 33)

Address	Description	Range	Step	Format	Default
00BE	Port 9 activity	0 to 1	1	F3	0
00BF	Port 10 activity	0 to 1	1	F3	0
00C0	Port 11 activity	0 to 1	1	F3	0
00C1	Port 12 activity	0 to 1	1	F3	0
00C2	Port 13 activity	0 to 1	1	F3	0
00C3	Port 14 activity	0 to 1	1	F3	0
00C4	Port 15 activity	0 to 1	1	F3	0
00C5	Port 16 activity	0 to 1	1	F3	0
00C6	Port 17 activity	0 to 1	1	F3	0
00C7	Port 18 activity	0 to 1	1	F3	0
00C8	Port 19 activity	0 to 1	1	F3	0
00C9	Port 20 activity	0 to 1	1	F3	0
00CA	Port 21 activity	0 to 1	1	F3	0
00CB	Port 22 activity	0 to 1	1	F3	0
00CC	Port 23 activity	0 to 1	1	F3	0
00CD	Port 24 activity	0 to 1	1	F3	0
00CE	Port 25 activity	0 to 1	1	F3	0
00CF	Port 26 activity	0 to 1	1	F3	0
00D0	Port 27 activity	0 to 1	1	F3	0
00D1	Port 28 activity	0 to 1	1	F3	0
00D2	Port 29 activity	0 to 1	1	F3	0
00D3	Port 30 activity	0 to 1	1	F3	0
00D4	Port 31 activity	0 to 1	1	F3	0
00D5	Port 32 activity	0 to 1	1	F3	0
00D6	Port 1: Number of bytes received	0 to 4294967295	1	F9	0
00D8	Port 1: Number of bytes sent	0 to 4294967295	1	F9	0
00DA	Port 1: Number of frames received	0 to 4294967295	1	F9	0
00DC	Port 1: Number of frames sent	0 to 4294967295	1	F9	0
00DE	Port 1: Total bytes received	0 to 4294967295	1	F9	0
00E0	Port 1: Total frames received	0 to 4294967295	1	F9	0
00E2	Port 1: Number of broadcast frames received	0 to 4294967295	1	F9	0
00E4	Port 1: Number of multicast frames received	0 to 4294967295	1	F9	0
00E6	Port 1: Number of frames with CRC error	0 to 4294967295	1	F9	0
00E8	Port 1: Number of oversized frames received	0 to 4294967295	1	F9	0
00EA	Port 1: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
00EC	Port 1: Number of jabber frames received	0 to 4294967295	1	F9	0
00EE	Port 1: Number of collisions occurred	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 5 of 33)

Address	Description	Range	Step	Format	Default
00F0	Port 1: Number of late collisions occurred	0 to 4294967295	1	F9	0
00F2	Port 1: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
00F4	Port 1: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
00F6	Port 1: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
00F8	Port 1: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
00FA	Port 1: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
00FC	Port 1: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
00FE	Port 1: Number of MAC error packets	0 to 4294967295	1	F9	0
0100	Port 1: Number of dropped received packets	0 to 4294967295	1	F9	0
0102	Port 1: Number of multicast frames sent	0 to 4294967295	1	F9	0
0104	Port 1: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0106	Port 1: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0108	Port 2: Number of bytes received	0 to 4294967295	1	F9	0
010A	Port 2: Number of bytes sent	0 to 4294967295	1	F9	0
010C	Port 2: Number of frames received	0 to 4294967295	1	F9	0
010E	Port 2: Number of frames sent	0 to 4294967295	1	F9	0
0110	Port 2: Total bytes received	0 to 4294967295	1	F9	0
0112	Port 2: Total frames received	0 to 4294967295	1	F9	0
0114	Port 2: Number of broadcast frames received	0 to 4294967295	1	F9	0
0116	Port 2: Number of multicast frames received	0 to 4294967295	1	F9	0
0118	Port 2: Number of frames with CRC error	0 to 4294967295	1	F9	0
011A	Port 2: Number of oversized frames received	0 to 4294967295	1	F9	0
011C	Port 2: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
011E	Port 2: Number of jabber frames received	0 to 4294967295	1	F9	0
0120	Port 2: Number of collisions occurred	0 to 4294967295	1	F9	0
0122	Port 2: Number of late collisions occurred	0 to 4294967295	1	F9	0
0124	Port 2: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0126	Port 2: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 6 of 33)

Address	Description	Range	Step	Format	Default
0128	Port 2: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
012A	Port 2: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
012C	Port 2: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
012E	Port 2: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0130	Port 2: Number of MAC error packets	0 to 4294967295	1	F9	0
0132	Port 2: Number of dropped received packets	0 to 4294967295	1	F9	0
0134	Port 2: Number of multicast frames sent	0 to 4294967295	1	F9	0
0136	Port 2: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0138	Port 2: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
013A	Port 3: Number of bytes received	0 to 4294967295	1	F9	0
013C	Port 3: Number of bytes sent	0 to 4294967295	1	F9	0
013E	Port 3: Number of frames received	0 to 4294967295	1	F9	0
0140	Port 3: Number of frames sent	0 to 4294967295	1	F9	0
0142	Port 3: Total bytes received	0 to 4294967295	1	F9	0
0144	Port 3: Total frames received	0 to 4294967295	1	F9	0
0146	Port 3: Number of broadcast frames received	0 to 4294967295	1	F9	0
0148	Port 3: Number of multicast frames received	0 to 4294967295	1	F9	0
014A	Port 3: Number of frames with CRC error	0 to 4294967295	1	F9	0
014C	Port 3: Number of oversized frames received	0 to 4294967295	1	F9	0
014E	Port 3: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0150	Port 3: Number of jabber frames received	0 to 4294967295	1	F9	0
0152	Port 3: Number of collisions occurred	0 to 4294967295	1	F9	0
0154	Port 3: Number of late collisions occurred	0 to 4294967295	1	F9	0
0156	Port 3: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0158	Port 3: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
015A	Port 3: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
015C	Port 3: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
015E	Port 3: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 7 of 33)

Address	Description	Range	Step	Format	Default
0160	Port 3: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0162	Port 3: Number of MAC error packets	0 to 4294967295	1	F9	0
0164	Port 3: Number of dropped received packets	0 to 4294967295	1	F9	0
0166	Port 3: Number of multicast frames sent	0 to 4294967295	1	F9	0
0168	Port 3: Number of broadcast frames sent	0 to 4294967295	1	F9	0
016A	Port 3: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
016C	Port 4: Number of bytes received	0 to 4294967295	1	F9	0
016E	Port 4: Number of bytes sent	0 to 4294967295	1	F9	0
0170	Port 4: Number of frames received	0 to 4294967295	1	F9	0
0172	Port 4: Number of frames sent	0 to 4294967295	1	F9	0
0174	Port 4: Total bytes received	0 to 4294967295	1	F9	0
0176	Port 4: Total frames received	0 to 4294967295	1	F9	0
0178	Port 4: Number of broadcast frames received	0 to 4294967295	1	F9	0
017A	Port 4: Number of multicast frames received	0 to 4294967295	1	F9	0
017C	Port 4: Number of frames with CRC error	0 to 4294967295	1	F9	0
017E	Port 4: Number of oversized frames received	0 to 4294967295	1	F9	0
0180	Port 4: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0182	Port 4: Number of jabber frames received	0 to 4294967295	1	F9	0
0184	Port 4: Number of collisions occurred	0 to 4294967295	1	F9	0
0186	Port 4: Number of late collisions occurred	0 to 4294967295	1	F9	0
0188	Port 4: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
018A	Port 4: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
018C	Port 4: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
018E	Port 4: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0190	Port 4: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0192	Port 4: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0194	Port 4: Number of MAC error packets	0 to 4294967295	1	F9	0
0196	Port 4: Number of dropped received packets	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 8 of 33)

Address	Description	Range	Step	Format	Default
0198	Port 4: Number of multicast frames sent	0 to 4294967295	1	F9	0
019A	Port 4: Number of broadcast frames sent	0 to 4294967295	1	F9	0
019C	Port 4: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
019E	Port 5: Number of bytes received	0 to 4294967295	1	F9	0
01A0	Port 5: Number of bytes sent	0 to 4294967295	1	F9	0
01A2	Port 5: Number of frames received	0 to 4294967295	1	F9	0
01A4	Port 5: Number of frames sent	0 to 4294967295	1	F9	0
01A6	Port 5: Total bytes received	0 to 4294967295	1	F9	0
01A8	Port 5: Total frames received	0 to 4294967295	1	F9	0
01AA	Port 5: Number of broadcast frames received	0 to 4294967295	1	F9	0
01AC	Port 5: Number of multicast frames received	0 to 4294967295	1	F9	0
01AE	Port 5: Number of frames with CRC error	0 to 4294967295	1	F9	0
01B0	Port 5: Number of oversized frames received	0 to 4294967295	1	F9	0
01B2	Port 5: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
01B4	Port 5: Number of jabber frames received	0 to 4294967295	1	F9	0
01B6	Port 5: Number of collisions occurred	0 to 4294967295	1	F9	0
01B8	Port 5: Number of late collisions occurred	0 to 4294967295	1	F9	0
01BA	Port 5: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
01BC	Port 5: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
01BE	Port 5: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
01C0	Port 5: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
01C2	Port 5: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
01C4	Port 5: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
01C6	Port 5: Number of MAC error packets	0 to 4294967295	1	F9	0
01C8	Port 5: Number of dropped received packets	0 to 4294967295	1	F9	0
01CA	Port 5: Number of multicast frames sent	0 to 4294967295	1	F9	0
01CC	Port 5: Number of broadcast frames sent	0 to 4294967295	1	F9	0
01CE	Port 5: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 9 of 33)

Address	Description	Range	Step	Format	Default
01D0	Port 6: Number of bytes received	0 to 4294967295	1	F9	0
01D2	Port 6: Number of bytes sent	0 to 4294967295	1	F9	0
01D4	Port 6: Number of frames received	0 to 4294967295	1	F9	0
01D6	Port 6: Number of frames sent	0 to 4294967295	1	F9	0
01D8	Port 6: Total bytes received	0 to 4294967295	1	F9	0
01DA	Port 6: Total frames received	0 to 4294967295	1	F9	0
01DC	Port 6: Number of broadcast frames received	0 to 4294967295	1	F9	0
01DE	Port 6: Number of multicast frames received	0 to 4294967295	1	F9	0
01E0	Port 6: Number of frames with CRC error	0 to 4294967295	1	F9	0
01E2	Port 6: Number of oversized frames received	0 to 4294967295	1	F9	0
01E4	Port 6: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
01E6	Port 6: Number of jabber frames received	0 to 4294967295	1	F9	0
01E8	Port 6: Number of collisions occurred	0 to 4294967295	1	F9	0
01EA	Port 6: Number of late collisions occurred	0 to 4294967295	1	F9	0
01EC	Port 6: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
01EE	Port 6: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
01F0	Port 6: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
01F2	Port 6: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
01F4	Port 6: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
01F6	Port 6: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
01F8	Port 6: Number of MAC error packets	0 to 4294967295	1	F9	0
01FA	Port 6: Number of dropped received packets	0 to 4294967295	1	F9	0
01FC	Port 6: Number of multicast frames sent	0 to 4294967295	1	F9	0
01FE	Port 6: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0200	Port 6: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0202	Port 7: Number of bytes received	0 to 4294967295	1	F9	0
0204	Port 7: Number of bytes sent	0 to 4294967295	1	F9	0
0206	Port 7: Number of frames received	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 10 of 33)

Address	Description	Range	Step	Format	Default
0208	Port 7: Number of frames sent	0 to 4294967295	1	F9	0
020A	Port 7: Total bytes received	0 to 4294967295	1	F9	0
020C	Port 7: Total frames received	0 to 4294967295	1	F9	0
020E	Port 7: Number of broadcast frames received	0 to 4294967295	1	F9	0
0210	Port 7: Number of multicast frames received	0 to 4294967295	1	F9	0
0212	Port 7: Number of frames with CRC error	0 to 4294967295	1	F9	0
0214	Port 7: Number of oversized frames received	0 to 4294967295	1	F9	0
0216	Port 7: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0218	Port 7: Number of jabber frames received	0 to 4294967295	1	F9	0
021A	Port 7: Number of collisions occurred	0 to 4294967295	1	F9	0
021C	Port 7: Number of late collisions occurred	0 to 4294967295	1	F9	0
021E	Port 7: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0220	Port 7: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0222	Port 7: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0224	Port 7: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0226	Port 7: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0228	Port 7: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
022A	Port 7: Number of MAC error packets	0 to 4294967295	1	F9	0
022C	Port 7: Number of dropped received packets	0 to 4294967295	1	F9	0
022E	Port 7: Number of multicast frames sent	0 to 4294967295	1	F9	0
0230	Port 7: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0232	Port 7: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0234	Port 8: Number of bytes received	0 to 4294967295	1	F9	0
0236	Port 8: Number of bytes sent	0 to 4294967295	1	F9	0
0238	Port 8: Number of frames received	0 to 4294967295	1	F9	0
023A	Port 8: Number of frames sent	0 to 4294967295	1	F9	0
023C	Port 8: Total bytes received	0 to 4294967295	1	F9	0
023E	Port 8: Total frames received	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 11 of 33)

Address	Description	Range	Step	Format	Default
0240	Port 8: Number of broadcast frames received	0 to 4294967295	1	F9	0
0242	Port 8: Number of multicast frames received	0 to 4294967295	1	F9	0
0244	Port 8: Number of frames with CRC error	0 to 4294967295	1	F9	0
0246	Port 8: Number of oversized frames received	0 to 4294967295	1	F9	0
0248	Port 8: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
024A	Port 8: Number of jabber frames received	0 to 4294967295	1	F9	0
024C	Port 8: Number of collisions occurred	0 to 4294967295	1	F9	0
024E	Port 8: Number of late collisions occurred	0 to 4294967295	1	F9	0
0250	Port 8: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0252	Port 8: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0254	Port 8: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0256	Port 8: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0258	Port 8: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
025A	Port 8: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
025C	Port 8: Number of MAC error packets	0 to 4294967295	1	F9	0
025E	Port 8: Number of dropped received packets	0 to 4294967295	1	F9	0
0260	Port 8: Number of multicast frames sent	0 to 4294967295	1	F9	0
0262	Port 8: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0264	Port 8: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0266	Port 9: Number of bytes received	0 to 4294967295	1	F9	0
0268	Port 9: Number of bytes sent	0 to 4294967295	1	F9	0
026A	Port 9: Number of frames received	0 to 4294967295	1	F9	0
026C	Port 9: Number of frames sent	0 to 4294967295	1	F9	0
026E	Port 9: Total bytes received	0 to 4294967295	1	F9	0
0270	Port 9: Total frames received	0 to 4294967295	1	F9	0
0272	Port 9: Number of broadcast frames received	0 to 4294967295	1	F9	0
0274	Port 9: Number of multicast frames received	0 to 4294967295	1	F9	0
0276	Port 9: Number of frames with CRC error	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 12 of 33)

Address	Description	Range	Step	Format	Default
0278	Port 9: Number of oversized frames received	0 to 4294967295	1	F9	0
027A	Port 9: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
027C	Port 9: Number of jabber frames received	0 to 4294967295	1	F9	0
027E	Port 9: Number of collisions occurred	0 to 4294967295	1	F9	0
0280	Port 9: Number of late collisions occurred	0 to 4294967295	1	F9	0
0282	Port 9: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0284	Port 9: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0286	Port 9: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0288	Port 9: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
028A	Port 9: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
028C	Port 9: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
028E	Port 9: Number of MAC error packets	0 to 4294967295	1	F9	0
0290	Port 9: Number of dropped received packets	0 to 4294967295	1	F9	0
0292	Port 9: Number of multicast frames sent	0 to 4294967295	1	F9	0
0294	Port 9: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0296	Port 9: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0298	Port 10: Number of bytes received	0 to 4294967295	1	F9	0
029A	Port 10: Number of bytes sent	0 to 4294967295	1	F9	0
029C	Port 10: Number of frames received	0 to 4294967295	1	F9	0
029E	Port 10: Number of frames sent	0 to 4294967295	1	F9	0
02A0	Port 10: Total bytes received	0 to 4294967295	1	F9	0
02A2	Port 10: Total frames received	0 to 4294967295	1	F9	0
02A4	Port 10: Number of broadcast frames received	0 to 4294967295	1	F9	0
02A6	Port 10: Number of multicast frames received	0 to 4294967295	1	F9	0
02A8	Port 10: Number of frames with CRC error	0 to 4294967295	1	F9	0
02AA	Port 10: Number of oversized frames received	0 to 4294967295	1	F9	0
02AC	Port 10: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
02AE	Port 10: Number of jabber frames received	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 13 of 33)

Address	Description	Range	Step	Format	Default
02B0	Port 10: Number of collisions occurred	0 to 4294967295	1	F9	0
02B2	Port 10: Number of late collisions occurred	0 to 4294967295	1	F9	0
02B4	Port 10: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
02B6	Port 10: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
02B8	Port 10: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
02BA	Port 10: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
02BC	Port 10: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
02BE	Port 10: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
02C0	Port 10: Number of MAC error packets	0 to 4294967295	1	F9	0
02C2	Port 10: Number of dropped received packets	0 to 4294967295	1	F9	0
02C4	Port 10: Number of multicast frames sent	0 to 4294967295	1	F9	0
02C6	Port 10: Number of broadcast frames sent	0 to 4294967295	1	F9	0
02C8	Port 10: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
02CA	Port 11: Number of bytes received	0 to 4294967295	1	F9	0
02CC	Port 11: Number of bytes sent	0 to 4294967295	1	F9	0
02CE	Port 11: Number of frames received	0 to 4294967295	1	F9	0
02D0	Port 11: Number of frames sent	0 to 4294967295	1	F9	0
02D2	Port 11: Total bytes received	0 to 4294967295	1	F9	0
02D4	Port 11: Total frames received	0 to 4294967295	1	F9	0
02D6	Port 11: Number of broadcast frames received	0 to 4294967295	1	F9	0
02D8	Port 11: Number of multicast frames received	0 to 4294967295	1	F9	0
02DA	Port 11: Number of frames with CRC error	0 to 4294967295	1	F9	0
02DC	Port 11: Number of oversized frames received	0 to 4294967295	1	F9	0
02DE	Port 11: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
02E0	Port 11: Number of jabber frames received	0 to 4294967295	1	F9	0
02E2	Port 11: Number of collisions occurred	0 to 4294967295	1	F9	0
02E4	Port 11: Number of late collisions occurred	0 to 4294967295	1	F9	0
02E6	Port 11: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 14 of 33)

Address	Description	Range	Step	Format	Default
02E8	Port 11: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
02EA	Port 11: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
02EC	Port 11: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
02EE	Port 11: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
02F0	Port 11: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
02F2	Port 11: Number of MAC error packets	0 to 4294967295	1	F9	0
02F4	Port 11: Number of dropped received packets	0 to 4294967295	1	F9	0
02F6	Port 11: Number of multicast frames sent	0 to 4294967295	1	F9	0
02F8	Port 11: Number of broadcast frames sent	0 to 4294967295	1	F9	0
02FA	Port 11: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
02FC	Port 12: Number of bytes received	0 to 4294967295	1	F9	0
02FE	Port 12: Number of bytes sent	0 to 4294967295	1	F9	0
0300	Port 12: Number of frames received	0 to 4294967295	1	F9	0
0302	Port 12: Number of frames sent	0 to 4294967295	1	F9	0
0304	Port 12: Total bytes received	0 to 4294967295	1	F9	0
0306	Port 12: Total frames received	0 to 4294967295	1	F9	0
0308	Port 12: Number of broadcast frames received	0 to 4294967295	1	F9	0
030A	Port 12: Number of multicast frames received	0 to 4294967295	1	F9	0
030C	Port 12: Number of frames with CRC error	0 to 4294967295	1	F9	0
030E	Port 12: Number of oversized frames received	0 to 4294967295	1	F9	0
0310	Port 12: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0312	Port 12: Number of jabber frames received	0 to 4294967295	1	F9	0
0314	Port 12: Number of collisions occurred	0 to 4294967295	1	F9	0
0316	Port 12: Number of late collisions occurred	0 to 4294967295	1	F9	0
0318	Port 12: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
031A	Port 12: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
031C	Port 12: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
031E	Port 12: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 15 of 33)

Address	Description	Range	Step	Format	Default
0320	Port 12: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0322	Port 12: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0324	Port 12: Number of MAC error packets	0 to 4294967295	1	F9	0
0326	Port 12: Number of dropped received packets	0 to 4294967295	1	F9	0
0328	Port 12: Number of multicast frames sent	0 to 4294967295	1	F9	0
032A	Port 12: Number of broadcast frames sent	0 to 4294967295	1	F9	0
032C	Port 12: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
032E	Port 13: Number of bytes received	0 to 4294967295	1	F9	0
0330	Port 13: Number of bytes sent	0 to 4294967295	1	F9	0
0332	Port 13: Number of frames received	0 to 4294967295	1	F9	0
0334	Port 13: Number of frames sent	0 to 4294967295	1	F9	0
0336	Port 13: Total bytes received	0 to 4294967295	1	F9	0
0338	Port 13: Total frames received	0 to 4294967295	1	F9	0
033A	Port 13: Number of broadcast frames received	0 to 4294967295	1	F9	0
033C	Port 13: Number of multicast frames received	0 to 4294967295	1	F9	0
033E	Port 13: Number of frames with CRC error	0 to 4294967295	1	F9	0
0340	Port 13: Number of oversized frames received	0 to 4294967295	1	F9	0
0342	Port 13: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0344	Port 13: Number of jabber frames received	0 to 4294967295	1	F9	0
0346	Port 13: Number of collisions occurred	0 to 4294967295	1	F9	0
0348	Port 13: Number of late collisions occurred	0 to 4294967295	1	F9	0
034A	Port 13: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
034C	Port 13: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
034E	Port 13: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0350	Port 13: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0352	Port 13: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0354	Port 13: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0356	Port 13: Number of MAC error packets	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 16 of 33)

Address	Description	Range	Step	Format	Default
0358	Port 13: Number of dropped received packets	0 to 4294967295	1	F9	0
035A	Port 13: Number of multicast frames sent	0 to 4294967295	1	F9	0
035C	Port 13: Number of broadcast frames sent	0 to 4294967295	1	F9	0
035E	Port 13: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0360	Port 14: Number of bytes received	0 to 4294967295	1	F9	0
0362	Port 14: Number of bytes sent	0 to 4294967295	1	F9	0
0364	Port 14: Number of frames received	0 to 4294967295	1	F9	0
0366	Port 14: Number of frames sent	0 to 4294967295	1	F9	0
0368	Port 14: Total bytes received	0 to 4294967295	1	F9	0
036A	Port 14: Total frames received	0 to 4294967295	1	F9	0
036C	Port 14: Number of broadcast frames received	0 to 4294967295	1	F9	0
036E	Port 14: Number of multicast frames received	0 to 4294967295	1	F9	0
0370	Port 14: Number of frames with CRC error	0 to 4294967295	1	F9	0
0372	Port 14: Number of oversized frames received	0 to 4294967295	1	F9	0
0374	Port 14: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0376	Port 14: Number of jabber frames received	0 to 4294967295	1	F9	0
0378	Port 14: Number of collisions occurred	0 to 4294967295	1	F9	0
037A	Port 14: Number of late collisions occurred	0 to 4294967295	1	F9	0
037C	Port 14: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
037E	Port 14: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0380	Port 14: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0382	Port 14: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0384	Port 14: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0386	Port 14: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0388	Port 14: Number of MAC error packets	0 to 4294967295	1	F9	0
038A	Port 14: Number of dropped received packets	0 to 4294967295	1	F9	0
038C	Port 14: Number of multicast frames sent	0 to 4294967295	1	F9	0
038E	Port 14: Number of broadcast frames sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 17 of 33)

Address	Description	Range	Step	Format	Default
0390	Port 14: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0392	Port 15: Number of bytes received	0 to 4294967295	1	F9	0
0394	Port 15: Number of bytes sent	0 to 4294967295	1	F9	0
0396	Port 15: Number of frames received	0 to 4294967295	1	F9	0
0398	Port 15: Number of frames sent	0 to 4294967295	1	F9	0
039A	Port 15: Total bytes received	0 to 4294967295	1	F9	0
039C	Port 15: Total frames received	0 to 4294967295	1	F9	0
039E	Port 15: Number of broadcast frames received	0 to 4294967295	1	F9	0
03A0	Port 15: Number of multicast frames received	0 to 4294967295	1	F9	0
03A2	Port 15: Number of frames with CRC error	0 to 4294967295	1	F9	0
03A4	Port 15: Number of oversized frames received	0 to 4294967295	1	F9	0
03A6	Port 15: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
03A8	Port 15: Number of jabber frames received	0 to 4294967295	1	F9	0
03AA	Port 15: Number of collisions occurred	0 to 4294967295	1	F9	0
03AC	Port 15: Number of late collisions occurred	0 to 4294967295	1	F9	0
03AE	Port 15: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
03B0	Port 15: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
03B2	Port 15: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
03B4	Port 15: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
03B6	Port 15: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
03B8	Port 15: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
03BA	Port 15: Number of MAC error packets	0 to 4294967295	1	F9	0
03BC	Port 15: Number of dropped received packets	0 to 4294967295	1	F9	0
03BE	Port 15: Number of multicast frames sent	0 to 4294967295	1	F9	0
03C0	Port 15: Number of broadcast frames sent	0 to 4294967295	1	F9	0
03C2	Port 15: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
03C4	Port 16: Number of bytes received	0 to 4294967295	1	F9	0
03C6	Port 16: Number of bytes sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 18 of 33)

Address	Description	Range	Step	Format	Default
03C8	Port 16: Number of frames received	0 to 4294967295	1	F9	0
03CA	Port 16: Number of frames sent	0 to 4294967295	1	F9	0
03CC	Port 16: Total bytes received	0 to 4294967295	1	F9	0
03CE	Port 16: Total frames received	0 to 4294967295	1	F9	0
03D0	Port 16: Number of broadcast frames received	0 to 4294967295	1	F9	0
03D2	Port 16: Number of multicast frames received	0 to 4294967295	1	F9	0
03D4	Port 16: Number of frames with CRC error	0 to 4294967295	1	F9	0
03D6	Port 16: Number of oversized frames received	0 to 4294967295	1	F9	0
03D8	Port 16: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
03DA	Port 16: Number of jabber frames received	0 to 4294967295	1	F9	0
03DC	Port 16: Number of collisions occurred	0 to 4294967295	1	F9	0
03DE	Port 16: Number of late collisions occurred	0 to 4294967295	1	F9	0
03E0	Port 16: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
03E2	Port 16: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
03E4	Port 16: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
03E6	Port 16: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
03E8	Port 16: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
03EA	Port 16: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
03EC	Port 16: Number of MAC error packets	0 to 4294967295	1	F9	0
03EE	Port 16: Number of dropped received packets	0 to 4294967295	1	F9	0
03F0	Port 16: Number of multicast frames sent	0 to 4294967295	1	F9	0
03F2	Port 16: Number of broadcast frames sent	0 to 4294967295	1	F9	0
03F4	Port 16: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
03F6	Port 17: Number of bytes received	0 to 4294967295	1	F9	0
03F8	Port 17: Number of bytes sent	0 to 4294967295	1	F9	0
03FA	Port 17: Number of frames received	0 to 4294967295	1	F9	0
03FC	Port 17: Number of frames sent	0 to 4294967295	1	F9	0
03FE	Port 17: Total bytes received	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 19 of 33)

Address	Description	Range	Step	Format	Default
0400	Port 17: Total frames received	0 to 4294967295	1	F9	0
0402	Port 17: Number of broadcast frames received	0 to 4294967295	1	F9	0
0404	Port 17: Number of multicast frames received	0 to 4294967295	1	F9	0
0406	Port 17: Number of frames with CRC error	0 to 4294967295	1	F9	0
0408	Port 17: Number of oversized frames received	0 to 4294967295	1	F9	0
040A	Port 17: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
040C	Port 17: Number of jabber frames received	0 to 4294967295	1	F9	0
040E	Port 17: Number of collisions occurred	0 to 4294967295	1	F9	0
0410	Port 17: Number of late collisions occurred	0 to 4294967295	1	F9	0
0412	Port 17: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0414	Port 17: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0416	Port 17: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0418	Port 17: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
041A	Port 17: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
041C	Port 17: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
041E	Port 17: Number of MAC error packets	0 to 4294967295	1	F9	0
0420	Port 17: Number of dropped received packets	0 to 4294967295	1	F9	0
0422	Port 17: Number of multicast frames sent	0 to 4294967295	1	F9	0
0424	Port 17: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0426	Port 17: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0428	Port 18: Number of bytes received	0 to 4294967295	1	F9	0
042A	Port 18: Number of bytes sent	0 to 4294967295	1	F9	0
042C	Port 18: Number of frames received	0 to 4294967295	1	F9	0
042E	Port 18: Number of frames sent	0 to 4294967295	1	F9	0
0430	Port 18: Total bytes received	0 to 4294967295	1	F9	0
0432	Port 18: Total frames received	0 to 4294967295	1	F9	0
0434	Port 18: Number of broadcast frames received	0 to 4294967295	1	F9	0
0436	Port 18: Number of multicast frames received	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 20 of 33)

Address	Description	Range	Step	Format	Default
0438	Port 18: Number of frames with CRC error	0 to 4294967295	1	F9	0
043A	Port 18: Number of oversized frames received	0 to 4294967295	1	F9	0
043C	Port 18: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
043E	Port 18: Number of jabber frames received	0 to 4294967295	1	F9	0
0440	Port 18: Number of collisions occurred	0 to 4294967295	1	F9	0
0442	Port 18: Number of late collisions occurred	0 to 4294967295	1	F9	0
0444	Port 18: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0446	Port 18: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0448	Port 18: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
044A	Port 18: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
044C	Port 18: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
044E	Port 18: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0450	Port 18: Number of MAC error packets	0 to 4294967295	1	F9	0
0452	Port 18: Number of dropped received packets	0 to 4294967295	1	F9	0
0454	Port 18: Number of multicast frames sent	0 to 4294967295	1	F9	0
0456	Port 18: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0458	Port 18: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
045A	Port 19: Number of bytes received	0 to 4294967295	1	F9	0
045C	Port 19: Number of bytes sent	0 to 4294967295	1	F9	0
045E	Port 19: Number of frames received	0 to 4294967295	1	F9	0
0460	Port 19: Number of frames sent	0 to 4294967295	1	F9	0
0462	Port 19: Total bytes received	0 to 4294967295	1	F9	0
0464	Port 19: Total frames received	0 to 4294967295	1	F9	0
0466	Port 19: Number of broadcast frames received	0 to 4294967295	1	F9	0
0468	Port 19: Number of multicast frames received	0 to 4294967295	1	F9	0
046A	Port 19: Number of frames with CRC error	0 to 4294967295	1	F9	0
046C	Port 19: Number of oversized frames received	0 to 4294967295	1	F9	0
046E	Port 19: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 21 of 33)

Address	Description	Range	Step	Format	Default
0470	Port 19: Number of jabber frames received	0 to 4294967295	1	F9	0
0472	Port 19: Number of collisions occurred	0 to 4294967295	1	F9	0
0474	Port 19: Number of late collisions occurred	0 to 4294967295	1	F9	0
0476	Port 19: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0478	Port 19: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
047A	Port 19: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
047C	Port 19: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
047E	Port 19: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0480	Port 19: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0482	Port 19: Number of MAC error packets	0 to 4294967295	1	F9	0
0484	Port 19: Number of dropped received packets	0 to 4294967295	1	F9	0
0486	Port 19: Number of multicast frames sent	0 to 4294967295	1	F9	0
0488	Port 19: Number of broadcast frames sent	0 to 4294967295	1	F9	0
048A	Port 19: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
048C	Port 20: Number of bytes received	0 to 4294967295	1	F9	0
048E	Port 20: Number of bytes sent	0 to 4294967295	1	F9	0
0490	Port 20: Number of frames received	0 to 4294967295	1	F9	0
0492	Port 20: Number of frames sent	0 to 4294967295	1	F9	0
0494	Port 20: Total bytes received	0 to 4294967295	1	F9	0
0496	Port 20: Total frames received	0 to 4294967295	1	F9	0
0498	Port 20: Number of broadcast frames received	0 to 4294967295	1	F9	0
049A	Port 20: Number of multicast frames received	0 to 4294967295	1	F9	0
049C	Port 20: Number of frames with CRC error	0 to 4294967295	1	F9	0
049E	Port 20: Number of oversized frames received	0 to 4294967295	1	F9	0
04A0	Port 20: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
04A2	Port 20: Number of jabber frames received	0 to 4294967295	1	F9	0
04A4	Port 20: Number of collisions occurred	0 to 4294967295	1	F9	0
04A6	Port 20: Number of late collisions occurred	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 22 of 33)

Address	Description	Range	Step	Format	Default
04A8	Port 20: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
04AA	Port 20: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
04AC	Port 20: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
04AE	Port 20: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
04B0	Port 20: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
04B2	Port 20: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
04B4	Port 20: Number of MAC error packets	0 to 4294967295	1	F9	0
04B6	Port 20: Number of dropped received packets	0 to 4294967295	1	F9	0
04B8	Port 20: Number of multicast frames sent	0 to 4294967295	1	F9	0
04BA	Port 20: Number of broadcast frames sent	0 to 4294967295	1	F9	0
04BC	Port 20: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
04BE	Port 21: Number of bytes received	0 to 4294967295	1	F9	0
04C0	Port 21: Number of bytes sent	0 to 4294967295	1	F9	0
04C2	Port 21: Number of frames received	0 to 4294967295	1	F9	0
04C4	Port 21: Number of frames sent	0 to 4294967295	1	F9	0
04C6	Port 21: Total bytes received	0 to 4294967295	1	F9	0
04C8	Port 21: Total frames received	0 to 4294967295	1	F9	0
04CA	Port 21: Number of broadcast frames received	0 to 4294967295	1	F9	0
04CC	Port 21: Number of multicast frames received	0 to 4294967295	1	F9	0
04CE	Port 21: Number of frames with CRC error	0 to 4294967295	1	F9	0
04D0	Port 21: Number of oversized frames received	0 to 4294967295	1	F9	0
04D2	Port 21: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
04D4	Port 21: Number of jabber frames received	0 to 4294967295	1	F9	0
04D6	Port 21: Number of collisions occurred	0 to 4294967295	1	F9	0
04D8	Port 21: Number of late collisions occurred	0 to 4294967295	1	F9	0
04DA	Port 21: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
04DC	Port 21: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
04DE	Port 21: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 23 of 33)

Address	Description	Range	Step	Format	Default
04E0	Port 21: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
04E2	Port 21: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
04E4	Port 21: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
04E6	Port 21: Number of MAC error packets	0 to 4294967295	1	F9	0
04E8	Port 21: Number of dropped received packets	0 to 4294967295	1	F9	0
04EA	Port 21: Number of multicast frames sent	0 to 4294967295	1	F9	0
04EC	Port 21: Number of broadcast frames sent	0 to 4294967295	1	F9	0
04EE	Port 21: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
04F0	Port 22: Number of bytes received	0 to 4294967295	1	F9	0
04F2	Port 22: Number of bytes sent	0 to 4294967295	1	F9	0
04F4	Port 22: Number of frames received	0 to 4294967295	1	F9	0
04F6	Port 22: Number of frames sent	0 to 4294967295	1	F9	0
04F8	Port 22: Total bytes received	0 to 4294967295	1	F9	0
04FA	Port 22: Total frames received	0 to 4294967295	1	F9	0
04FC	Port 22: Number of broadcast frames received	0 to 4294967295	1	F9	0
04FE	Port 22: Number of multicast frames received	0 to 4294967295	1	F9	0
0500	Port 22: Number of frames with CRC error	0 to 4294967295	1	F9	0
0502	Port 22: Number of oversized frames received	0 to 4294967295	1	F9	0
0504	Port 22: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0506	Port 22: Number of jabber frames received	0 to 4294967295	1	F9	0
0508	Port 22: Number of collisions occurred	0 to 4294967295	1	F9	0
050A	Port 22: Number of late collisions occurred	0 to 4294967295	1	F9	0
050C	Port 22: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
050E	Port 22: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0510	Port 22: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0512	Port 22: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0514	Port 22: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0516	Port 22: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 24 of 33)

Address	Description	Range	Step	Format	Default
0518	Port 22: Number of MAC error packets	0 to 4294967295	1	F9	0
051A	Port 22: Number of dropped received packets	0 to 4294967295	1	F9	0
051C	Port 22: Number of multicast frames sent	0 to 4294967295	1	F9	0
051E	Port 22: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0520	Port 22: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0522	Port 23: Number of bytes received	0 to 4294967295	1	F9	0
0524	Port 23: Number of bytes sent	0 to 4294967295	1	F9	0
0526	Port 23: Number of frames received	0 to 4294967295	1	F9	0
0528	Port 23: Number of frames sent	0 to 4294967295	1	F9	0
052A	Port 23: Total bytes received	0 to 4294967295	1	F9	0
052C	Port 23: Total frames received	0 to 4294967295	1	F9	0
052E	Port 23: Number of broadcast frames received	0 to 4294967295	1	F9	0
0530	Port 23: Number of multicast frames received	0 to 4294967295	1	F9	0
0532	Port 23: Number of frames with CRC error	0 to 4294967295	1	F9	0
0534	Port 23: Number of oversized frames received	0 to 4294967295	1	F9	0
0536	Port 23: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0538	Port 23: Number of jabber frames received	0 to 4294967295	1	F9	0
053A	Port 23: Number of collisions occurred	0 to 4294967295	1	F9	0
053C	Port 23: Number of late collisions occurred	0 to 4294967295	1	F9	0
053E	Port 23: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0540	Port 23: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0542	Port 23: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0544	Port 23: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0546	Port 23: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0548	Port 23: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
054A	Port 23: Number of MAC error packets	0 to 4294967295	1	F9	0
054C	Port 23: Number of dropped received packets	0 to 4294967295	1	F9	0
054E	Port 23: Number of multicast frames sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 25 of 33)

Address	Description	Range	Step	Format	Default
0550	Port 23: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0552	Port 23: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0554	Port 24: Number of bytes received	0 to 4294967295	1	F9	0
0556	Port 24: Number of bytes sent	0 to 4294967295	1	F9	0
0558	Port 24: Number of frames received	0 to 4294967295	1	F9	0
055A	Port 24: Number of frames sent	0 to 4294967295	1	F9	0
055C	Port 24: Total bytes received	0 to 4294967295	1	F9	0
055E	Port 24: Total frames received	0 to 4294967295	1	F9	0
0560	Port 24: Number of broadcast frames received	0 to 4294967295	1	F9	0
0562	Port 24: Number of multicast frames received	0 to 4294967295	1	F9	0
0564	Port 24: Number of frames with CRC error	0 to 4294967295	1	F9	0
0566	Port 24: Number of oversized frames received	0 to 4294967295	1	F9	0
0568	Port 24: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
056A	Port 24: Number of jabber frames received	0 to 4294967295	1	F9	0
056C	Port 24: Number of collisions occurred	0 to 4294967295	1	F9	0
056E	Port 24: Number of late collisions occurred	0 to 4294967295	1	F9	0
0570	Port 24: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0572	Port 24: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0574	Port 24: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0576	Port 24: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0578	Port 24: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
057A	Port 24: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
057C	Port 24: Number of MAC error packets	0 to 4294967295	1	F9	0
057E	Port 24: Number of dropped received packets	0 to 4294967295	1	F9	0
0580	Port 24: Number of multicast frames sent	0 to 4294967295	1	F9	0
0582	Port 24: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0584	Port 24: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0586	Port 25: Number of bytes received	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 26 of 33)

Address	Description	Range	Step	Format	Default
0588	Port 25: Number of bytes sent	0 to 4294967295	1	F9	0
058A	Port 25: Number of frames received	0 to 4294967295	1	F9	0
058C	Port 25: Number of frames sent	0 to 4294967295	1	F9	0
058E	Port 25: Total bytes received	0 to 4294967295	1	F9	0
0590	Port 25: Total frames received	0 to 4294967295	1	F9	0
0592	Port 25: Number of broadcast frames received	0 to 4294967295	1	F9	0
0594	Port 25: Number of multicast frames received	0 to 4294967295	1	F9	0
0596	Port 25: Number of frames with CRC error	0 to 4294967295	1	F9	0
0598	Port 25: Number of oversized frames received	0 to 4294967295	1	F9	0
059A	Port 25: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
059C	Port 25: Number of jabber frames received	0 to 4294967295	1	F9	0
059E	Port 25: Number of collisions occurred	0 to 4294967295	1	F9	0
05A0	Port 25: Number of late collisions occurred	0 to 4294967295	1	F9	0
05A2	Port 25: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
05A4	Port 25: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
05A6	Port 25: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
05A8	Port 25: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
05AA	Port 25: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
05AC	Port 25: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
05AE	Port 25: Number of MAC error packets	0 to 4294967295	1	F9	0
05B0	Port 25: Number of dropped received packets	0 to 4294967295	1	F9	0
05B2	Port 25: Number of multicast frames sent	0 to 4294967295	1	F9	0
05B4	Port 25: Number of broadcast frames sent	0 to 4294967295	1	F9	0
05B6	Port 25: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
05B8	Port 26: Number of bytes received	0 to 4294967295	1	F9	0
05BA	Port 26: Number of bytes sent	0 to 4294967295	1	F9	0
05BC	Port 26: Number of frames received	0 to 4294967295	1	F9	0
05BE	Port 26: Number of frames sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 27 of 33)

Address	Description	Range	Step	Format	Default
05C0	Port 26: Total bytes received	0 to 4294967295	1	F9	0
05C2	Port 26: Total frames received	0 to 4294967295	1	F9	0
05C4	Port 26: Number of broadcast frames received	0 to 4294967295	1	F9	0
05C6	Port 26: Number of multicast frames received	0 to 4294967295	1	F9	0
05C8	Port 26: Number of frames with CRC error	0 to 4294967295	1	F9	0
05CA	Port 26: Number of oversized frames received	0 to 4294967295	1	F9	0
05CC	Port 26: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
05CE	Port 26: Number of jabber frames received	0 to 4294967295	1	F9	0
05D0	Port 26: Number of collisions occurred	0 to 4294967295	1	F9	0
05D2	Port 26: Number of late collisions occurred	0 to 4294967295	1	F9	0
05D4	Port 26: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
05D6	Port 26: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
05D8	Port 26: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
05DA	Port 26: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
05DC	Port 26: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
05DE	Port 26: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
05E0	Port 26: Number of MAC error packets	0 to 4294967295	1	F9	0
05E2	Port 26: Number of dropped received packets	0 to 4294967295	1	F9	0
05E4	Port 26: Number of multicast frames sent	0 to 4294967295	1	F9	0
05E6	Port 26: Number of broadcast frames sent	0 to 4294967295	1	F9	0
05E8	Port 26: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
05EA	Port 27: Number of bytes received	0 to 4294967295	1	F9	0
05EC	Port 27: Number of bytes sent	0 to 4294967295	1	F9	0
05EE	Port 27: Number of frames received	0 to 4294967295	1	F9	0
05F0	Port 27: Number of frames sent	0 to 4294967295	1	F9	0
05F2	Port 27: Total bytes received	0 to 4294967295	1	F9	0
05F4	Port 27: Total frames received	0 to 4294967295	1	F9	0
05F6	Port 27: Number of broadcast frames received	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 28 of 33)

Address	Description	Range	Step	Format	Default
05F8	Port 27: Number of multicast frames received	0 to 4294967295	1	F9	0
05FA	Port 27: Number of frames with CRC error	0 to 4294967295	1	F9	0
05FC	Port 27: Number of oversized frames received	0 to 4294967295	1	F9	0
05FE	Port 27: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0600	Port 27: Number of jabber frames received	0 to 4294967295	1	F9	0
0602	Port 27: Number of collisions occurred	0 to 4294967295	1	F9	0
0604	Port 27: Number of late collisions occurred	0 to 4294967295	1	F9	0
0606	Port 27: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0608	Port 27: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
060A	Port 27: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
060C	Port 27: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
060E	Port 27: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0610	Port 27: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0612	Port 27: Number of MAC error packets	0 to 4294967295	1	F9	0
0614	Port 27: Number of dropped received packets	0 to 4294967295	1	F9	0
0616	Port 27: Number of multicast frames sent	0 to 4294967295	1	F9	0
0618	Port 27: Number of broadcast frames sent	0 to 4294967295	1	F9	0
061A	Port 27: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
061C	Port 28: Number of bytes received	0 to 4294967295	1	F9	0
061E	Port 28: Number of bytes sent	0 to 4294967295	1	F9	0
0620	Port 28: Number of frames received	0 to 4294967295	1	F9	0
0622	Port 28: Number of frames sent	0 to 4294967295	1	F9	0
0624	Port 28: Total bytes received	0 to 4294967295	1	F9	0
0626	Port 28: Total frames received	0 to 4294967295	1	F9	0
0628	Port 28: Number of broadcast frames received	0 to 4294967295	1	F9	0
062A	Port 28: Number of multicast frames received	0 to 4294967295	1	F9	0
062C	Port 28: Number of frames with CRC error	0 to 4294967295	1	F9	0
062E	Port 28: Number of oversized frames received	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 29 of 33)

Address	Description	Range	Step	Format	Default
0630	Port 28: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0632	Port 28: Number of jabber frames received	0 to 4294967295	1	F9	0
0634	Port 28: Number of collisions occurred	0 to 4294967295	1	F9	0
0636	Port 28: Number of late collisions occurred	0 to 4294967295	1	F9	0
0638	Port 28: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
063A	Port 28: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
063C	Port 28: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
063E	Port 28: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0640	Port 28: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0642	Port 28: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0644	Port 28: Number of MAC error packets	0 to 4294967295	1	F9	0
0646	Port 28: Number of dropped received packets	0 to 4294967295	1	F9	0
0648	Port 28: Number of multicast frames sent	0 to 4294967295	1	F9	0
064A	Port 28: Number of broadcast frames sent	0 to 4294967295	1	F9	0
064C	Port 28: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
064E	Port 29: Number of bytes received	0 to 4294967295	1	F9	0
0650	Port 29: Number of bytes sent	0 to 4294967295	1	F9	0
0652	Port 29: Number of frames received	0 to 4294967295	1	F9	0
0654	Port 29: Number of frames sent	0 to 4294967295	1	F9	0
0656	Port 29: Total bytes received	0 to 4294967295	1	F9	0
0658	Port 29: Total frames received	0 to 4294967295	1	F9	0
065A	Port 29: Number of broadcast frames received	0 to 4294967295	1	F9	0
065C	Port 29: Number of multicast frames received	0 to 4294967295	1	F9	0
065E	Port 29: Number of frames with CRC error	0 to 4294967295	1	F9	0
0660	Port 29: Number of oversized frames received	0 to 4294967295	1	F9	0
0662	Port 29: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0664	Port 29: Number of jabber frames received	0 to 4294967295	1	F9	0
0666	Port 29: Number of collisions occurred	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 30 of 33)

Address	Description	Range	Step	Format	Default
0668	Port 29: Number of late collisions occurred	0 to 4294967295	1	F9	0
066A	Port 29: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
066C	Port 29: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
066E	Port 29: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0670	Port 29: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0672	Port 29: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
0674	Port 29: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
0676	Port 29: Number of MAC error packets	0 to 4294967295	1	F9	0
0678	Port 29: Number of dropped received packets	0 to 4294967295	1	F9	0
067A	Port 29: Number of multicast frames sent	0 to 4294967295	1	F9	0
067C	Port 29: Number of broadcast frames sent	0 to 4294967295	1	F9	0
067E	Port 29: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0680	Port 30: Number of bytes received	0 to 4294967295	1	F9	0
0682	Port 30: Number of bytes sent	0 to 4294967295	1	F9	0
0684	Port 30: Number of frames received	0 to 4294967295	1	F9	0
0686	Port 30: Number of frames sent	0 to 4294967295	1	F9	0
0688	Port 30: Total bytes received	0 to 4294967295	1	F9	0
068A	Port 30: Total frames received	0 to 4294967295	1	F9	0
068C	Port 30: Number of broadcast frames received	0 to 4294967295	1	F9	0
068E	Port 30: Number of multicast frames received	0 to 4294967295	1	F9	0
0690	Port 30: Number of frames with CRC error	0 to 4294967295	1	F9	0
0692	Port 30: Number of oversized frames received	0 to 4294967295	1	F9	0
0694	Port 30: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
0696	Port 30: Number of jabber frames received	0 to 4294967295	1	F9	0
0698	Port 30: Number of collisions occurred	0 to 4294967295	1	F9	0
069A	Port 30: Number of late collisions occurred	0 to 4294967295	1	F9	0
069C	Port 30: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
069E	Port 30: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 31 of 33)

Address	Description	Range	Step	Format	Default
06A0	Port 30: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
06A2	Port 30: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
06A4	Port 30: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
06A6	Port 30: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
06A8	Port 30: Number of MAC error packets	0 to 4294967295	1	F9	0
06AA	Port 30: Number of dropped received packets	0 to 4294967295	1	F9	0
06AC	Port 30: Number of multicast frames sent	0 to 4294967295	1	F9	0
06AE	Port 30: Number of broadcast frames sent	0 to 4294967295	1	F9	0
06B0	Port 30: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
06B2	Port 31: Number of bytes received	0 to 4294967295	1	F9	0
06B4	Port 31: Number of bytes sent	0 to 4294967295	1	F9	0
06B6	Port 31: Number of frames received	0 to 4294967295	1	F9	0
06B8	Port 31: Number of frames sent	0 to 4294967295	1	F9	0
06BA	Port 31: Total bytes received	0 to 4294967295	1	F9	0
06BC	Port 31: Total frames received	0 to 4294967295	1	F9	0
06BE	Port 31: Number of broadcast frames received	0 to 4294967295	1	F9	0
06C0	Port 31: Number of multicast frames received	0 to 4294967295	1	F9	0
06C2	Port 31: Number of frames with CRC error	0 to 4294967295	1	F9	0
06C4	Port 31: Number of oversized frames received	0 to 4294967295	1	F9	0
06C6	Port 31: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
06C8	Port 31: Number of jabber frames received	0 to 4294967295	1	F9	0
06CA	Port 31: Number of collisions occurred	0 to 4294967295	1	F9	0
06CC	Port 31: Number of late collisions occurred	0 to 4294967295	1	F9	0
06CE	Port 31: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
06D0	Port 31: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
06D2	Port 31: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
06D4	Port 31: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
06D6	Port 31: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 32 of 33)

Address	Description	Range	Step	Format	Default
06D8	Port 31: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
06DA	Port 31: Number of MAC error packets	0 to 4294967295	1	F9	0
06DC	Port 31: Number of dropped received packets	0 to 4294967295	1	F9	0
06DE	Port 31: Number of multicast frames sent	0 to 4294967295	1	F9	0
06E0	Port 31: Number of broadcast frames sent	0 to 4294967295	1	F9	0
06E2	Port 31: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
06E4	Port 32: Number of bytes received	0 to 4294967295	1	F9	0
06E6	Port 32: Number of bytes sent	0 to 4294967295	1	F9	0
06E8	Port 32: Number of frames received	0 to 4294967295	1	F9	0
06EA	Port 32: Number of frames sent	0 to 4294967295	1	F9	0
06EC	Port 32: Total bytes received	0 to 4294967295	1	F9	0
06EE	Port 32: Total frames received	0 to 4294967295	1	F9	0
06F0	Port 32: Number of broadcast frames received	0 to 4294967295	1	F9	0
06F2	Port 32: Number of multicast frames received	0 to 4294967295	1	F9	0
06F4	Port 32: Number of frames with CRC error	0 to 4294967295	1	F9	0
06F6	Port 32: Number of oversized frames received	0 to 4294967295	1	F9	0
06F8	Port 32: Number of bad fragments received (<64 bytes)	0 to 4294967295	1	F9	0
06FA	Port 32: Number of jabber frames received	0 to 4294967295	1	F9	0
06FC	Port 32: Number of collisions occurred	0 to 4294967295	1	F9	0
06FE	Port 32: Number of late collisions occurred	0 to 4294967295	1	F9	0
0700	Port 32: Number of 64-byte frames received/sent	0 to 4294967295	1	F9	0
0702	Port 32: Number of 65 to 127 byte frames received/sent	0 to 4294967295	1	F9	0
0704	Port 32: Number of 128 to 255 byte frames received/sent	0 to 4294967295	1	F9	0
0706	Port 32: Number of 256 to 511 byte frames received/sent	0 to 4294967295	1	F9	0
0708	Port 32: Number of 512 to 1023 byte frames received/sent	0 to 4294967295	1	F9	0
070A	Port 32: Number of 1023 to maximum byte frames received/sent	0 to 4294967295	1	F9	0
070C	Port 32: Number of MAC error packets	0 to 4294967295	1	F9	0
070E	Port 32: Number of dropped received packets	0 to 4294967295	1	F9	0

Table 18–1: Modbus memory map (Sheet 33 of 33)

Address	Description	Range	Step	Format	Default
0710	Port 32: Number of multicast frames sent	0 to 4294967295	1	F9	0
0712	Port 32: Number of broadcast frames sent	0 to 4294967295	1	F9	0
0714	Port 32: Number of <64 byte fragments with good CRC	0 to 4294967295	1	F9	0
0716	Serial Number	---	---	String	Varies

18.2.2 Format Codes

- **Bitmap**: 32-bit group of bits, packed into two registers. Encoded in big endian.
- **F1**: 16-bit unsigned integer
- **F2**: Enumeration - power alarm

  0 = power supply good
  1 = power supply fail
- **F3**: Enumeration - OFF/ON

  0 = Off
  1 = On
- **F4**: Enumeration: port type

  0 = Giga - GBIC
  1 = Copper - TP
  2 = Fiber - 10
  3 = Fiber - 100
  4 = Giga - 10/100/1000 (triple speed)
  5 = Giga - Copper 1000 TP
  6 = Giga - SFP
- **F9**: 32-bit unsigned long
- **String**: A sequence of octets, packed 2 to one register in sequence.

Multilink ML2400

Ethernet Communications Switch

Chapter 19: Appendix

19.1 Revision History

19.1.1 Change Notes

Table 19–1: Revision history

Part Number	Revision	Release Date	ECO
1601-0220-A1	1.5.1	06 May 2005	---
1601-0220-A2	1.5.1	19 May 2005	---
1601-0220-A3	1.5.1	11 July 2005	---
1601-0220-A4	1.5.1	16 September 2005	---
1601-0220-A5	1.6.1	08 June 2006	---
1601-0220-A6	1.7.x	18 August 2006	---
1601-0220-A7	1.7.x	9 January 2007	---
1601-0220-A8	1.7.x	24 January 2007	---
1601-0220-A9	1.7.x	25 May 2007	---
1601-0220-AA	2.0.x	20 October 2007	---
1601-0220-AB	3.x	27 June 2008	---

19.1.2 Changes to the Manual

Table 19–2: Updates for Manual Revision AB

Section	Description
General	Manual revised to AB
General	Firmware release revised to 3.x

Table 19–3: Updates for Manual Revision AA

Section	Description
General	Manual revised to AA
General	Firmware release revised to 2.0.x
1.2.1	Order Code table revised
1.3.3	Added Type Tests section
5.5	IPv6 section added
5.4.2, 5.4.3, 5,4,4	Improved Configuration sections (3) added
Table 4-2	Corrections to table
Table 18-1	Add one new RAW to table - address 0716

Table 19–4: Updates for Manual Revision A9

Section	Description
1.2.1	Changes to reflect addition of three new modules
General	Manual revised to A9

Table 19–5: Updates for Manual Revision A7

Section	Description
1.2.1	Change power supply ranges in Order Codes section
1.3.1	Description of Power Input Ranges in Input Voltage and Input Current sections
1.3.1	Add short-term temperature duration (-40 to 85 degC for 16 hours)
1.3.2	Ambient Temperature Standard from IEC 60068 to IEC60068-2-1 and IEC60068-2-2
1.3.4	Add UL information: Ul listed/recognized; Change to CE Standard EN50082-1 and remove EN55024:1998
3.3.1	Table-top/shelf-mounted model name is ML2400-AC
3.4.1	Add filter ground symbol where "filter ground" text appears
3.4.4	Revised picture
3.4.2	Add note #6 (For AC and HI powered units...) to UL Requirements section
12.1	Remove Link Loss Learn section
General	Firmware Revision updated to 1.7.x
General	Manual revised to A7

Table 19–6: Updates for 1601-0220-A6

Page (A5)	Page (A6)	Change	Description
Title	Title	Update	Manual revision to A6
1-2	1-2	Update	Updated *Ordering* section
1-3	1-3	Update	Updated *Power Supply* specifications
9-7	9-7	Update	Updated *Link Loss Alert* section

Table 19–7: Updates for 1601-0220-A5

Page (A4)	Page (A5)	Change	Description
Title	Title	Update	Manual revision to A5
1-2	1-2	Update	Updated *Ordering* section
1-3	1-3	Update	Updated *Power Supply* specifications
---	1-6	Add	Added *Automatic IP Address Configuration* section
2-1	2-1	Update	Updated *Communication Modules* section
4-3	4-3	Update	Updated *Power Budget Calculations with Fiber Media* section
5-2	5-2	Update	Updated *Configuring DHCP/ BOOTP/Manual* section
10-12	10-12	Update	Updated *Configuring Tag VLANs with EnerVista* section
13-10	13-10	Update	Updated *Configuring STP/RSTP with EnerVista* section
17-11	17-11	Update	Updated *Command List* section (now called *Command Reference*)

Table 19–8: Major updates for 1601-0220-A4 (Sheet 1 of 2)

Page (A3)	Page (A4)	Change	Description
Title	Title	Update	Manual revision to A4

Table 19–8: Major updates for 1601-0220-A4 (Sheet 2 of 2)

Page (A3)	Page (A4)	Change	Description
1-3	1-3	Update	Updated Power Supply specifications

Table 19–9: Major updates for 1601-0220-A3

Page (A2)	Page (A3)	Change	Description
Title	Title	Update	Manual revision to A3
1-3	1-3	Update	Updated Power Supply specifications

Table 19–10: Major updates for 1601-0220-A2

Page (A1)	Page (A2)	Change	Description
Title	Title	Update	Manual revision to A2
1-2	1-2	Update	Updated order code table
2-3	2-3	Update	Updated Gigabit module diagram
3-4	3-4	Update	Updated the POWERING THE ML2400 section
3-4	3-4	Remove	Removed the REDUNDANT POWER SUPPLY section

19.2 Warranty

19.2.1 GE Multilin Warranty Statement

General Electric Multilin Inc. (GE Multilin) warrants each switch it manufactures to be free from defects in material and workmanship under normal use and service for a period of 24 months from date of shipment from factory.

In the event of a failure covered by warranty, GE Multilin will undertake to repair or replace the relay providing the warrantor determined that it is defective and it is returned with all transportation charges prepaid to an authorized service centre or the factory. Repairs or replacement under warranty will be made without charge.

Warranty shall not apply to any relay which has been subject to misuse, negligence, accident, incorrect installation or use not in accordance with instructions nor any unit that has been altered outside a GE Multilin authorized factory outlet.

GE Multilin is not liable for special, indirect or consequential damages or for loss of profit or for expenses sustained as a result of a relay malfunction, incorrect application or adjustment.

For complete text of Warranty (including limitations and disclaimers), refer to GE Multilin Standard Conditions of Sale.

Index

Numerics

802.1X 7-1, 7-4

A

ALARM CONTACT 3-9
ALARM RELAY 2-8, 17-1
  specifications 1-4
APPLICATIONS 2-10
APPROVALS 1-6
AUTHORIZED MANAGERS 6-10
AUTO-NEGOTIATION 4-2

B

BACK PRESSURE 9-5
BOOTP 5-3
BRODCAST STORMS 9-8

C

CABLE LOSSES 4-5
CHANGES TO MANUAL 19-3, 19-4
CONNECTORS 1-3

D

DATE 5-9
DESIGN ASPECTS 2-2
DHCP 5-3
DIFFSERV 14-2

E

ELECTRICAL INSTALLATION 3-8
E-MAIL NOTIFICATION 16-2, 17-8
ENVIRONMENTAL SPECIFICATIONS 1-5
ETHERNET
  connecting 3-3
  modules 2-3
  power budget calculations 4-5
  specifications 1-3
EVENT LOG 17-15

F

FCC APPROVAL 1-6
FEATURES 2-7
FILTERING 4-1
FLOW CONTROL 2-7, 4-3, 9-5
FORWARDING 4-1
FRAME BUFFERING 2-7
FUNCTIONALITY 4-1

G

GARP 11-1
GVRP 11-1, 11-3

H

HISTORY 17-12

I

IEEE APPROVAL 1-6
IGMP 15-1, 15-2, 15-5
INSTALLATION 3-1
IP ADDRESSING 5-1
IP PRECEDENCE 14-2

L

LEDS
  functionality 4-2
  specifications 1-4
LINK LOSS ALERT 9-10

M

MAC ADDRESS 6-6
MECHANICAL INSTALLATION 3-6
MEMORY MAP 18-3
MODBUS
  configuration 18-1
  memory map 18-3
MODULES
  8-port copper 2-4
  combo modules 2-3, 2-4
  four-port fiber 2-3
  gigabit 2-6
MOUNTING
  specifications 1-6

N

NETWORK TIME 5-10

O

ORDER CODES 1-2

P

PACKET PRIORITIZATION 2-7
PASSWORDS 6-1
PING 17-13
PORT MIRRORING 9-1
PORT SETUP 9-3
PORT VLAN 10-4
PORT WEIGHT 14-5
POWER BUDGET CALCULATIONS 4-5
POWER SUPPLY
  specifications 1-4
PRODUCT DESCRIPTION 2-1

Q

QOS 2-7, 14-1, 14-4, 14-6, 14-9

R

RADIUS 7-1
REDUNDANT POWER SUPPLY 2-8
REVISION HISTORY 19-1
RSTP 13-1, 13-4, 13-7, 13-10

S

SAVING CONFIGURATION 5-13
SECURITY 6-1, 6-3, 6-5
SECURITY LOGS 6-9
SERIAL CONNECTIVITY 17-11
SERIAL PORT
  parameters 5-8
SMART RSTP 13-15
SMTP 17-6
SNMP 16-1, 16-6
SNTP 5-10
SOFTWARE 2-7
SPECIFICATIONS 1-3
STP 12-1, 12-3, 12-8
SWITCHING FUNCTIONALITY 4-1
SYSTEM EVENTS 17-15
SYSTEM INFORMATION 5-1

SYSTEM PARAMETERS 5-8

T

TACACS 7-1
TACACS+ 8-1
TAG VLAN 10-13
TELNET 5-5
TIME 5-9
TROUBLESHOOTING 4-7

U

UL REQUIREMENTS FOR DC UNITS 3-8
UNPACKING THE SWITCH 1-1
UP-LINK SWITCH 4-2

V

VLAN 10-1, 10-4, 10-13

W

WARRANTY 1-1, 1-7, 19-5